N. N. Worobjow

Teilbarkeitskriterien

Übersetzung: W. Arnold, L. Boll, D. Böttcher
1972 Deutscher Verlag der Wissenschaften
MSB: Nr. 52
Abschrift und LaTex-Satz: 2021 https://mathematikalpha.de

Vorwort

welches der Autor besonders aufmerksam zu lesen empfiehlt

Die moderne Mathematikausbildung in der Schule orientiert sich hauptsächlich auf die Erziehung der Schüler zum funktionalen Denken und zur Fähigkeit, mit kontinuierlichen mathematischen Objekten umzugehen. Die vielfach vorgenommenen Veränderungen in den Lehrplänen für Mathematik weisen in dieselbe Richtung.
Nun wurden aber in der letzten Zeit neue Gebiete der Anwendung mathematischer Kenntnisse erschlossen wie das Aufstellen von Programmen für Rechenautomaten, Aspekte der Kybernetik und Operationsforschung, mathematische Ökonomik, mathematische Linguistik und so weiter. Die Beherrschung dieser Gebiete der Wissenschaft sowie die Vervollkommnung des klassischen Apparates erfordern die Entwicklung einer kombinatorischen Technik, der Analysis des Diskreten und die Schaffung neuer fruchtbarer Abstraktionen. Deshalb müssen die genannten Aspekte der Mathematik auch in der populärwissenschaftlichen Literatur behandelt werden.

Vom Waldrand führen viele Pfade ins Dickicht. Sie sind verschlungen, laufen zusammen, gehen wieder auseinander und kreuzen sich. Bei einem Spaziergang wird man nur die Vielzahl dieser Pfade bemerken, einige von ihnen betreten und ihre Richtung in die Tiefe des Waldes verfolgen. Will man den Wald gründlicher kennenlernen, so muss man die unterschiedlichsten Pfade entlanggehen, so lange sie überhaupt noch unter trockenen Nadeln und Heidelbeersträuchern erkennbar sind.
Um sich die Gaben des Waldes zunutze zu machen, muss man die gangbaren Wege aber überhaupt verlassen und sich einen Weg durch das Geflecht dorniger Zweige bahnen.

Die vorliegende Broschüre kann als Beschreibung eines der möglichen Spaziergänge am Rande der modernen Mathematik angesehen werden. Die Darlegung grundlegender Dinge, die sich auf Teilbarkeitskriterien beziehen, erlaubt es, einige ziemlich abstrakte Fragen der diskreten Mathematik zu berühren.
Dazu gehören vor allem die Aussagen der elementaren Zahlentheorie, die sich um den Hauptsatz der Arithmetik und die kanonische Zerlegung einer natürlichen Zahl in Primfaktoren gruppieren. Ferner wird die Teilbarkeit der Zahlen selbst als Relation über der Menge der ganzen Zahlen betrachtet, d. h. als Verwirklichung eines ziemlich abstrakten allgemeinen Begriffes.
Schließlich werden die Teilbarkeitskriterien hier als Algorithmen behandelt, die jede Zahl daraufhin untersuchen, ob sie durch eine gegebene Zahl teilbar ist oder nicht. Der Autor hielt es für zweckmäßig, unter den Teilbarkeitskriterien besonders die Restklassenkriterien hervorzuheben, welche die Zahlen bei Division durch eine gegebene Zahl in ihre Reste überführen.

Um die Wechselbeziehungen zwischen mathematischen Tatsachen hervorzuheben und zu zeigen, wie an ein- und denselben Gegenstand auf verschiedene Art und. Weise herangegangen werden kann, werden einige Aussagen zweimal, auf verschiedenen Wegen, bewiesen.

Das Büchlein ist für mathematikinteressierte Schüler der oberen Klassen bestimmt und

setzt, von einigen Anwendungen des binomischen Satzes abgesehen, keinerlei Vorkenntnisse voraus außer der Fähigkeit, einige einfache identische Umformungen vornehmen zu können. Die logische Struktur des Stoffes dagegen ist kompliziert, so dass seine Aneignung in allen Einzelheiten viel Aufmerksamkeit und Geduld erfordert.

Dem Leser sei folgender Plan für das Studium dieses Büchleins empfohlen:

Bei der ersten Lektüre sollte er sich lediglich auf den Haupttext der Paragraphen 1 bis 3 beschränken und keine Aufgaben lösen (mit Ausnahme der Aufgaben 31, 33, 35, 41, 43, 45, 46).
Das wird ihn mit dem Stoff sozusagen propädeutisch bekannt machen. Da die meisten in der Mathematik unbewanderten Menschen von der Richtigkeit des Satzes über die Eindeutigkeit der Zerlegung einer natürlichen Zahl in Primfaktoren überzeugt sind, ihn gewissermaßen für ein Axiom halten, können sie die Sätze 9 bis 13 als Folgerungen daraus auffassen.

Beim zweiten Studium sollte man versuchen, selbständig alle Sätze in der angeführten Reihenfolge zu beweisen.
Damit der Leser nicht zu oft der Versuchung erliegt, die fertigen Beweise der Sätze zu benutzen, wurden diese alle in einem besonderen Abschnitt zusammengefasst. Eine Ausnahme bildet der Beweis des Satzes 7, welcher - einer Stimmgabel vergleichbar - den Leser bereits beim ersten Lesen auf das erforderliche Niveau an mathematischer Strenge einstimmt.

Beim zweiten Lesen müssten der Paragraph 4 studiert und auch die Aufgaben des Haupttextes gelöst werden.
Beim dritten Lesen schließlich sollten das Kleingedruckte sowie die dazu gehörenden Aufgaben studiert werden.

Der Leser, der seine Kenntnisse auf dem Gebiet der Zahlentheorie, der abstrakten Relationentheorie oder schließlich der Theorie der Algorithmen vertiefen möchte, sei auf das Literaturverzeichnis am Ende des Büchleins verwiesen.

N. N. Worobjow

Inhaltsverzeichnis

1 Die Teilbarkeit von Zahlen

1. Summe, Differenz und Produkt zweier ganzer Zahlen sind ebenfalls ganze Zahlen. Dieser Sachverhalt wird im allgemeinen als Abgeschlossenheit der Menge der ganzen Zahlen hinsichtlich der Grundrechenarten Addition, Subtraktion und Multiplikation bezeichnet.
In Bezug auf die Division ist die Menge der ganzen Zahlen jedoch nicht abgeschlossen, denn der Quotient einer ganzen Zahl durch eine andere ganze Zahl ist im allgemeinen keine ganze Zahl.

Daher ergibt sich beim Betrachten der Division ganzer Zahlen als erstes die Frage nach der Ausführbarkeit dieser Grundrechenart für zwei gegebene Zahlen, d. h. die Frage nach der Teilbarkeit dieser Zahlen.
Bei der Betrachtung der übrigen arithmetischen Grundrechenarten mit ganzen Zahlen taucht eine entsprechende Frage offensichtlich nicht auf.

Im folgenden werden wir die wesentlichen Eigenschaften der arithmetischen Operationen mit ganzen Zahlen und auch die einfachsten Eigenschaften von Gleichungen und Ungleichungen als allgemein bekannt voraussetzen. Als "Zahl" ist dabei immer eine ganze Zahl gemeint, wenn nicht ausdrücklich etwas anderes gesagt wird.
Wie üblich werden die ganzen nichtnegativen Zahlen 0, 1, 2, ... als natürliche Zahlen bezeichnet. Wenn wir von allen natürlichen Zahlen sprechen, werden wir die Bezeichnung Menge der natürlichen Zahlen benutzen.

Definition. Die Zahl a ist teilbar durch die Zahl b (oder, was das gleiche ist, die Zahl b teilt die Zahl a), wenn es eine solche Zahl c gibt, dass $a = bc$ gilt.

Dieser Sachverhalt wird als Teilbarkeit der Zahl a durch die Zahl b bezeichnet und durch $b|a$ ausgedrückt.
Wir betonen, dass die Schreibweise $b|a$ nicht etwa eine Rechenoperation bedeutet, die mit den Zahlen a und b auszuführen ist, sondern eine Aussage über diese Zahlen. Je nachdem, wie die Zahlen a und b beschaffen sind, kann die Aussage $b|a$ richtig oder falsch sein. So ist beispielsweise die Aussage $2|4$ wahr, aber die Aussage $3|4$ falsch.

Um festzustellen, ob die Aussage $b|a$ @ wahr ist oder nicht, d. h., ob die Zahl a durch die Zahl b teilbar ist, gibt es eine Reihe verschiedener Verfahren. Eines davon besteht einfach darin, die Zahl a durch die Zahl b zu dividieren.
Das ist jedoch oft ziemlich langwierig und ermüdend. Naturgemäß möchte man sich von der Ausführbarkeit der Division überzeugen, ohne die Division wirklich durchführen zu müssen.
Auch ist folgende Überlegung nicht überflüssig: Uns interessiert eigentlich nur die Tatsache, ob die Zahl a durch die Zahl b teilbar ist; wenn wir aber die Division tatsächlich ausführen, erhalten wir nebenbei den Quotienten dieser Division und den Rest (wenn die Division "nicht aufgeht"); diese beiden Zahlen sind für uns jedoch ohne Belang, weil uns ja im Augenblick nur interessiert, ob der Rest gleich Null ist oder nicht.

Es besteht also Grund zu der Annahme, dass wir beim Ausführen der Division einen Teil der Arbeit (und offenbar keinen kleinen) darauf verwendet haben, Nebenprodukte

herzustellen. Man kann hoffen, dass es direktere Verfahren zur Klärung der Teilbarkeit gibt als die "primitive" Division, welche nicht so viele Nebenprodukte liefern, welche Ökonomischer sind und uns ermöglichen, schneller zu erkennen, ob Teilbarkeit vorliegt oder nicht. Diese Hoffnung geht in Erfüllung, und entsprechende Verfahren zur Klärung des Problems der Teilbarkeit existieren tatsächlich. Sie werden Teilbarkeitskriterien genannt.

Einige dieser Teilbarkeitskriterien sind dem Leser zweifellos bekannt. Das Ziel dieses Büchleins ist nun die hauptsächlich prinzipielle Untersuchung verschiedener Teilbarkeitskriterien.

Das Wesen jedes Kriteriums für die Teilbarkeit durch eine gegebene Zahl b besteht darin, dass mit seiner Hilfe die Frage, ob eine beliebige Zahl a durch b teilbar ist, auf das Problem zurückgeführt wird, ob eine Zahl kleiner als a durch b teilbar ist. (Es ist leicht zu sehen, dass das Verfahren, die Teilbarkeit mittels der üblichen Division festzustellen, ebenfalls auf diesem Gedanken beruht.)

Somit ist ein Teilbarkeitskriterium ein mathematisches Objekt von weit verbreiteter, aber unauffälliger Art. Es ist keine Formel, kein Satz, keine Definition, sondern ein Verfahren, etwa von der Art wie das Verfahren, Zahlen schriftlich zu multiplizieren, oder etwa das Verfahren, die Glieder einer arithmetischen Folge nacheinander zu berechnen.

Den Begriff des Teilbarkeitskriteriums werden wir im nächsten Abschnitt präzisieren.

2. In der Definition der Teilbarkeit von Zahlen ist nichts darüber gesagt, wieviel verschiedene Werte der Quotient bei Division von a durch b haben kann. Diese Frage werden wir hier ausführlich behandeln, um später nicht darauf eingehen zu müssen.

Es sei

$$a = bc \tag{1}$$

und außerdem

$$a = bc_1$$

Aus diesen Gleichungen erhalten wir

$$bc = bc_1 \qquad \text{oder} \qquad b(c - c_1) = 0$$

Ist b $\neq 0$, dann ist $c - c_1 = 0$, also $c = c_1$. Ist aber $b = 0$, so ist offenbar auch $a = 0$, und die Gleichung (1) ist für jedes c erfüllt.

Also ist nur Null durch Null teilbar, und der Wert dieses Quotienten ist unbestimmt. Gerade das ist gemeint, wenn man sagt, durch Null könne man nicht dividieren. Ist jedoch der Divisor von Null verschieden und die Division ausführbar, so hat der Quotient einen wohlbestimmten Wert.
Wenn im folgenden von Division die Rede ist, werden wir den Divisor immer als von Null verschieden annehmen.

Wir stellen hier die einfachsten Eigenschaften der Teilbarkeitsrelation zusammen.

Satz 1. Es gilt $a|a$.

Diese Eigenschaft der Teilbarkeitsrelation wird Reflexivität genannt.

Satz 2. Aus $b|a$ und $c|b$ folgt $c|a$.

Diese Eigenschaft der Teilbarkeitsrelation wird Transitivität genannt.

Satz 3. Gilt $b|a$ und $a|b$, so gilt entweder $a = b$ oder $a = -b$ (Antisymmetrie der Teilbarkeitsrelation).

Satz 4. Aus $b|a$ und $|b| > |a|$ folgt $a = 0$.

Folgerung. Aus $b|a$ und $a \neq 0$ folgt $|a| \geq |b|$.

Satz 5. Es gilt genau dann $b|a$, wenn $|b||a|$ gilt.

Aufgrund dieses Satzes können wir uns im folgenden auf den Fall beschränken, dass der Divisor eine positive Zahl ist.

Satz 6. Aus $b|a_1$, $b|a_2|$, ..., $b|a_n$ folgt

$$b|(a_1 + a_2 + ... + a_n)$$

Folgerung. Ist die Summe zweier Zahlen und einer ihrer Summanden durch eine Zahl b teilbar, so ist auch der andere Summand durch b teilbar.

Man darf nicht annehmen, diese Sätze seien offenkundig und bedürften keines besonderen Beweises. Es geht hier sogar nicht darum, dass in der Mathematik außer Axiomen und Definitionen alle Aussagen eines Beweises bedürfen. Die Beweise dieser Tatsachen (beispielsweise der, dass jede Zahl durch sich selbst teilbar ist) sind prinzipiell notwendig, weil sie nicht einfach aus der Definition der Teilbarkeit folgen, sondern auf Eigenschaften der Zahlen selbst beruhen.

Das folgende Beispiel wird uns das verdeutlichen.
Offenbar sind Summe, Differenz und Produkt von geraden Zahlen immer gerade. Die Division einer geraden Zahl durch eine andere gerade Zahl dagegen ist nicht immer ausführbar, und wenn sie es ist, braucht der Quotient nicht gerade zu sein. Daher kann man den Begriff der geradzahligen Teilbarkeit gerader Zahlen einführen.

Definition. Eine Zahl a heißt geradzahlig teilbar durch eine gerade Zahl b, wenn eine solche gerade Zahl c existiert, dass $a = bc$ gilt.

Offenbar gilt für die geradzahlige Teilbarkeit der Satz 1 nicht. Es gibt nämlich keine gerade Zahl c, für die $a = ac$ gilt.

Auf weitere Fragen, die mit der geradzahligen Teilbarkeit gerader Zahlen zusammenhängen, werden wir noch einige Male zurückkommen. Das Beispiel der geradzahligen Teilbarkeit zeigt, dass man verschiedene Teilbarkeitstheorien mit unterschiedlichen Eigenschaften aufstellen kann. Sätze, die für eine dieser Theorien gelten, brauchen für andere nicht richtig zu sein.

Aufgaben. Man beweise folgende Aussagen:
1. $a|0$.

2. $1|a$.
3. Aus $a|1$ folgt $a = \pm 1$.
4. Zu jedem $a \neq 0$ existiert eine von a verschiedene Zahl b, für welche $a|b$ gilt.
5. Zu jeder Zahl a existiert eine Zahl b derart, dass aus $c|b$ und $a|c$ entweder $c = b$ oder $c = a$ folgt.
6. Man beweise für die geradzahlige Teilbarkeit die den Sätzen 2, 3, 4 und 5 analogen Sätze.
7. Man formuliere eine Teilbarkeitstheorie, in welcher die Sätze 1, 3 und 4 gelten, nicht aber die Sätze 2 und 6.

3. Schon bei flüchtiger Betrachtung der konkreten Eigenschaften der Teilbarkeitsrelation fällt noch etwas auf: Die Teilbarkeit von Zahlen ist praktisch von deren Größe unabhängig.
Einerseits gibt es kleine Zahlen, die durch eine relativ große Anzahl von Zahlen teilbar sind. Zum Beispiel ist 12 durch die Zahlen 1, 2, 3, 4, 6 und 12 teilbar; die Zahl 60 hat zwölf Teiler. Solchen an Teilern reichen Zahlen kann man sehr große Zahlen gegenüberstellen, die die Minimalzahl von Teilern - nämlich zwei - haben (nach Satz 1 und Aufgabe 2 ist jede von 1 verschiedene Zahl durch mindestens zwei verschiedene Zahlen teilbar).
Es sind zwar bestimmte Gesetzmäßigkeiten bekannt, die die Teilbarkeit von Zahlen mit deren Größe verknüpfen, doch sind diese so kompliziert und verwickelt, dass wir sie hier nicht berühren werden.

4. Um so interessanter ist die Tatsache, dass es die Teilbarkeit an sich ermöglicht, die Zahlen in bestimmter Weise zu ordnen, wobei diese Ordnung von der gewöhnlichen - der Größe nach - abweicht, aber mit ihr vieles gemeinsam hat.
Überlegen wir einmal genau, was es eigentlich bedeutet, wenn wir sagen, man könne die natürlichen Zahlen ihrer Größe nach ordnen. Man versteht darunter, dass für bestimmte Zahlenpaare a, b eine Ordnungsbeziehung ("größer oder gleich")

$$a \geq b$$

besteht ; das soll heißen, die Differenz $a - b$ sei nicht negativ (d.h., es existiere eine natürliche Zahl c derart, dass $a = b + c$ ist).
Das Wesen der Teilbarkeit besteht nun ebenfalls darin, dass bestimmte Paare von Zahlen a und b einer ganz bestimmten Bedingung genügen (nämlich der, dass eine ganze Zahl c existiert, für die $a = bc$ gilt).

Somit sind die Teilbarkeitsrelation und die Relation "größer oder gleich" Begriffe ein und derselben Art. Daher kann man von ihren gemeinsamen Eigenschaften sprechen oder sie einander gegenüberstellen.

Insbesondere ist die Ordnungsrelation "größer oder gleich" zwischen zwei natürlichen Zahlen analog der Teilbarkeitsrelation eine bestimmte Aussage über diese Zahlen, die wahr oder falsch sein kann. (Zum Beispiel ist die Beziehung $5 \geq 3$ wahr, aber die Beziehung $3 \geq 5$ falsch.)

Wir bemerken sofort, dass die Relation "größer oder gleich" mehr gemeinsame Eigen-

schaften mit der Teilbarkeitsrelation hat als die Relation "größer als". Das hängt damit zusammen, dass die Relation "größer oder gleich" ähnlich der Teilbarkeitsrelation reflexiv ist (denn die Beziehung $a \geq a$ gilt für jedes a), aber die Relation "größer als" nicht reflexiv ist (denn die Ungleichung $a > a$ gilt ja nie).
Gerade deshalb wird hier als Ordnungsbeziehung zwischen natürlichen Zahlen die Relation "größer oder gleich" und nicht die scheinbar einfachere Relation "größer als" betrachtet.

5. Die Relation $\geq$ besitzt folgende leicht nachprüfbare Eigenschaften:

1. $a \geq$ a (Reflexivität).
2. Aus $a \geq b$ und $b \geq a$ folgt $a = b$ (Antisymmetrie).
3. Aus $a \geq b$ und $b \geq c$ folgt $a \geq c$ (Transitivität).
4. In jeder Folge natürlicher Zahlen

$$a_1 \geq a_2 \geq ... \geq a_n \geq ...$$

deren Glieder sämtlich voneinander verschieden sind, gibt es eine letzte Zahl. Diese Eigenschaft der Relation $\geq$ nennt man manchmal die Wohlordnungseigenschaft der Menge der natürlichen Zahlen.

Die Wohlordnungseigenschaft ist ziemlich kompliziert formuliert und sieht ein wenig gekünstelt aus. Sie erschließt jedoch außerordentlich wichtige Züge der Struktur der durch die Beziehung geordneten Menge der natürlichen Zahlen. Daraus lassen sich viele andere Eigenschaften dieser Relation folgern; wir werden sehen, dass gerade darauf solche in verschiedenen Gebieten der Mathematik benutzten Überlegungen wie die vollständige Induktion beruhen.

Als eine nützliche Anwendung dieser Eigenschaft erwähnen wir die folgende: Es gibt eine Zahl a derart, dass aus $a \geq b$ sogar $a = b$ folgt (hier sind a und $bnat\ddot{u}rlicheZahlen$).
Wenn es nämlich keine solche Zahl gäbe, könnten wir zu jedem a_n ein a_{n+1} finden derart, dass $a_n \geq a_{n+1}$ und $a_n \neq a_{n+1}$ wäre. Beginnend mit einem willkürlich gewählten a_1 erhielten wir die unendliche Folge aus verschiedenen Zahlen -

$$a_1 \geq a_2 \geq ... \geq a_n \geq a_{n+1} \geq ...$$

Die Existenz einer solchen Folge widerspricht aber der Wohlordnungseigenschaft der Menge der natürlichen Zahlen.
Somit existiert die genannte Zahl a tatsächlich. Sie heißt erste Zahl oder Minimalzahl (offenbar ist es die Null). Wir möchten hier jedoch bemerken, dass wir nicht bewiesen haben, dass diese Minimalzahl eindeutig bestimmt ist. Diese Eindeutigkeit wird im weiteren indirekt festgestellt.

5. Zu jeden Zahl a gibt es eine von a verschiedene Zahl b, für welche $b \geq a$ gilt. Diese Eigenschaft der natürlichen Zahlen heißt ihre Unbeschränktheit im Sinne der Relation $\geq$.

6. Zu jeder Zahl a, die nicht Minimalzahl ist, gibt es ein solches b, dass $a \geq b$, $a \neq b$ gilt und für jede Zahl c mit $a \geq c \geq b$ entweder $c = a$ oder $c = b$ folgt.

Diese formale Aussage bedeutet inhaltlich, dass jede natürliche Zahl außer der Null einen unmittelbaren natürlichen Vorgänger hat. (Man kann das auch so formulieren: Unter allen Zahlen, die kleiner als eine gegebene Zahl sind, gibt es eine größte.)

7. Es gilt entweder $a \geq b$ oder $b \geq a$. Diese Eigenschaft nennt man Dichotomie. In der Mathematik besagt dieses Wort, dass von zwei Möglichkeiten eine unbedingt realisiert wird. Das Wort selbst ist griechischen Ursprungs und bedeutet "Zweiteilung".

Wir betonen, dass die Aussagen 1 bis 7 Eigenschaften einer Relation über der Menge aller natürlicher Zahlen sind und nicht Eigenschaften irgendwelcher Zahlen, die durch diese Relationen verknüpft sind. Daher kann es vorkommen, dass sich für irgendeine andere Relation, welche Zahlen paarweise, aber nicht ihrer Größe nach, sondern auf andere Weise verknüpft, einige der Aussagen 1 bis 7 als falsch herausstellen.

Aufgabe 8. Man beweise ausschließlich unter Benutzung der Aussagen 1 bis 7 über die Relation $\geq$ und ohne Zuhilfenahme irgendwelcher Eigenschaften der Zahlen oder von Rechenoperationen

a) die Eindeutigkeit der Minimalzahl,
b) die Eindeutigkeit des unmittelbaren Vorgängers.
c) Man formuliere die Definition des unmittelbaren Nachfolgers einer Zahl a (d.h. der Zahl $a + 1$) und beweise seine Existenz und eindeutige Bestimmtheit.

Aufgabe 9. Man stelle fest, welche der Aussagen 1 bis 7 auch für die Relation "größer" ($>$) gelten.

6. Die Gültigkeit von Eigenschaften der Relation $\geq$ (wie übrigens jeder anderen auch) kann auf zweierlei Art gezeigt werden. Erstens können wir Eigenschaften irgendwelcher Zahlen oder bekannte Besonderheiten der Struktur der Menge der natürlichen Zahlen verwenden. In dieser Weise haben wir die Aussagen 1 bis 7 verifiziert.
Zweitens können wir, wenn wir uns von der Richtigkeit der Aussagen l bis 7 überzeugt haben, daraus ableiten, dass die Relation $\geq$ Zahlen paarweise verknüpft, und die weiteren Eigenschaften dieser Relation ausschließlich aus den Aussagen 1 bis 7 folgern. So wurden von uns die Existenz der Minimalzahl und die Aussagen der Aufgabe 8 bewiesen.

Der zweite Zugang zu einem Problem wird in der modernen Mathematik sehr häufig benutzt, man nennt ihn die axiomatische Methode.
Bei einem solchen Ansatz werden bestimmte Axiome aufgestellt (in unserem Fall sind es die Aussagen 1 bis 7), welche die Grundeigenschaften der zu untersuchenden Objekte widerspiegeln und ohne Beweis an den Anfang der Theorie gestellt werden. Daraus lassen sich alle übrigen Aussagen durch rein logisches Schließen folgern, ohne dass auf Eigenschaften der zu untersuchenden Objekte zurückgegriffen zu werden braucht. Diese Aussagen werden dann Sätze genannt.

Vielleicht erscheint einigen meiner Leser die Untersuchung von Eigenschaften von Relationen, losgelöst von den durch diese Relationen verknüpften Objekten, als die höchste mathematische Abstraktion, die im praktischen Leben völlig unnötig sei. In diesem Zu-

sammenhang seien zwei Bemerkungen gestattet.

Erstens: Vom Standpunkt der modernen Mathematik aus betrachtet, sind alle hier durchgeführten Überlegungen keineswegs "besonders abstrakt". Überdies müssen die Mathematiker unserer Zeit gleichzeitig viele Relationen untersuchen und sogar(!) Paare verschiedener Relationen durch neue Relationen, sogenannte "Relationen höherer Ordnung" verknüpfen.
Der bisher dargelegte Stoff gestattet es, den Begriff der Relation zwischen Relationen durch ein Beispiel zu veranschaulichen.

Es sei $\alpha, \beta, ...$ ein System von Relationen, welche natürliche Zahlen verknüpfen. Das bedeutet, dass wir für jedes Paar von Zahlen a und b und jede Relation γ aus unserem System wissen, ob das Paar a, b durch die Relation γ verknüpft ist oder nicht. Wenn a mit b durch die Relation γ verknüpft ist, wollen wir $a\gamma b$ schreiben.

Wir sagen, die Relation α sei stärker als die Relation β, und schreiben $\alpha \supset \beta$, wenn jedes Paar von Zahlen, das durch β verknüpft ist, auch durch die Relation α verknüpft ist, d. h., wenn aus $a\beta b$ auch $a\alpha b$ folgt.

Bezeichnen wir zum Beispiel die Relation der geradzahligen Teilbarkeit mit $|_g$, so können wir $| \supset |_g$ schreiben. Ferner ist offensichtlich $\geq \supset >$.
Dagegen gilt weder $| \supset \geq$ noch $\geq \supset |$. Die Teilbarkeitsrelation und die Relation "größer oder gleich" sind nicht durch die Relation $\supset$ verknüpft. Ein solcher Sachverhalt wurde im Abschnitt 3 beschrieben. (Teilbarkeit und Größe von Zahlen sind nicht durch eine Relation verknüpft.)
Natürlich erfordert das freie Operieren mit so komplizierten Begriffen wie einer Relation zwischen Relationen besondere Übung.

Zweitens: Derartige und sogar noch abstraktere Überlegungen treten immer öfter bei der Anwendung der Mathematik auf Ökonomie, Biologie, Linguistik oder das Militärwesen auf. Leider würden uns ausführlichere Betrachtungen darüber zu weit von unserem Hauptanliegen wegführen.

7. Damit, dass die Menge der natürlichen Zahlen durch die Relation $\geq$ geordnet werden kann, hängt die Tatsache zusammen, dass die Methode der vollständigen Induktion möglich ist. Gewöhnlich wird diese Methode in folgender Form angewandt:

Es sei $A(n)$ eine bestimmte Aussage, die eine beliebige natürliche Zahl n betrifft. Das bedeutet im Grunde genommen, dass wir es mit einer unendlichen Folge von Aussagen

$$A(0), A(1), ..., A(n), ...$$

über jede natürliche Zahl zu tun haben. Wir setzen voraus; dass

a) die Aussage $A(0)$ gilt (Basis der Induktion)[1]);
b) aus der Gültigkeit der Aussage $A(n)$ die Gültigkeit der Aussage $A(n+1)$ folgt (Induktionsschritt).

[1] Oft wird als Induktionsbasis auch $A(1)$ genommen. Das ist unwesentlich. Wichtig ist nur, dass sich die Basis der Induktion auf die erste der zu untersuchenden Zahlen bezieht.

Das Prinzip der vollständigen Induktion garantiert, dass unter den Voraussetzungen a) und b) die Aussage $A(n)$ für jedes natürliche n gilt.

Das Prinzip der vollständigen Induktion ist nicht etwa irgendeine selbständige Behauptung, sondern lässt sich aus den Eigenschaften 1 bis 7 der durch die Relation $\geq$ geordneten Menge der natürlichen Zahlen folgern.

Nehmen wir nämlich einmal an, die Voraussetzungen a) und b) des Induktionsprinzips für die Aussage $A(n)$ seien erfüllt, die Schlussfolgerung jedoch nicht. Letzteres bedeutet, dass Zahlen m existieren müssen, für welche die Aussage $A(m)$ nicht gilt. Es sei m_1 eine dieser Zahlen.
Wenn für alle $n < m_1$ die Aussage $A(n)$ gilt, ist m_1 die kleinste der Zahlen, für welche $A(n)$ nicht gilt. Wenn jedoch $A(n)$ nicht für alle $n < m_1$ gilt, muss ein $m_2 < m_1$ existieren, für das $A(m_2)$ nicht gilt.
Im Endergebnis kommen wir zu einer Folge verschiedener Zahlen

$$m_1 \geq m_2 \geq ... \geq m_r \geq ... \tag{2}$$

für welche $A(m)$ nicht gilt. Nach der Wohlordnungseigenschaft 4 muss in der Folge (2) ein letztes Glied m_r existieren. Offenbar ist m_r die kleinste aller Zahlen n, für die $A(n)$ nicht gilt.

Da $A(0)$ nach Voraussetzung wahr ist, muss $m_r \neq 0$ sein, so dass eine Zahl m_r^* existiert, die der unmittelbare Vorgänger von m_r ist (in Wirklichkeit ist dies $m_r - 1$). Da $m_r^* < m_r$ ist, muss die Aussage $A(m_r^*)$ gelten.
Nach der Bedingung b) des Induktionsprinzips muss dann auch die Aussage $A(m_r^* + 1)$, also auch $A(m_r)$ gelten.
Wir haben einen Widerspruch erhalten. Dieser Widerspruch zeigt, dass es keine Zahlen m gibt, für welche $A(m)$ nicht gilt. Also gilt $A(m)$ für alle Zahlen.

Wir wollen folgendes festhalten: Die soeben angestellten Überlegungen dürfen weder als Beweis des Induktionsprinzips noch als Begründung betrachtet werden. Sie weisen lediglich auf die Möglichkeit hin, eine mathematische Aussage (Methode der vollständigen Induktion) aus anderen (den Eigenschaften der Relation ;) zu folgern.
Diese Eigenschaften wurden von uns als Axiome angenommen und deshalb nicht bewiesen, sondern nur verifiziert. Jeder Versuch ihres mathematischen Beweises würde unvermeidlich dazu führen, dass irgendwelche neuen Voraussetzungen als Axiome eingeführt werden müssen.

Insbesondere muss man, um die Wohlordnungseigenschaft zu beweisen, die gleichen induktiven Überlegungen anstellen (der Leser kann sich selbst davon überzeugen).

Die Methode der vollständigen Induktion und verschiedene ihrer Varianten werden in den Bändchen von Sominski, Die Methode der vollständigen Induktion, und Golowina / Jaglom, Die Induktion in der Geometrie, (vgl. das Literaturverzeichnis) ausführlich mit vielen Beispielen behandelt. Auch wir werden sie hier mehrfach verwenden.

Aufgabe 10. Gegeben seien Paare von Objekten beliebiger Natur (das können Zahlen,

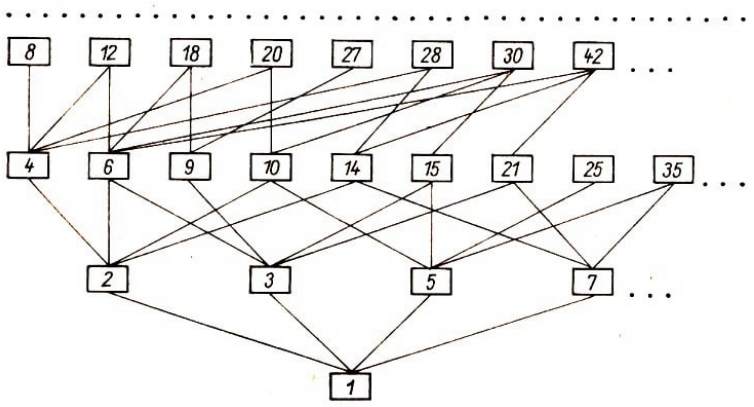
Funktionen, Punkte, Sätze usw. sein), die durch eine Relation $\succ$ verknüpft sind, welche Eigenschaften besitzt, die den Aussagen 1 bis 7 analog sind.
Man beweise, dass man dann diese Objekte (Elemente) nummerieren (d. h. in einer bestimmten Ordnung schreiben) kann: $A_1, A_2, A_3, ...$, so dass $A_i \succ A_j$, genau dann gilt, wenn $i \geq j$ ist.

Im Grunde bedeutet das, dass eine Relation, für welche die Aussagen 1 bis 7 gelten, eine Menge zu einer linearen Kette von Elementen ordnet:

$$A_1 \succ A_2 \succ A_3 \succ ...$$

8. Wir wollen jedoch zur Teilbarkeitsrelation zurückkehren. Wie die Sätze 1, 2 und 3 und die Aufgaben 3, 4 und. 5 zeigen, können wir für positive Zahlen in den Aussagen 1 bis 6 die Relation $\geq$ durch die Relation $|$ ersetzen.
Was jedoch die Aussage 7 betrifft, so lautet sie in Bezug auf die Teilbarkeit: "Von zwei Zahlen ist wenigstens eine durch die andere teilbar." Das ist aber nicht wahr.

Somit besitzt die Teilbarkeitsrelation alle Eigenschaften der Ordnung bis auf eine Ausnahme. Daraus lässt sich ableiten, dass die Teilbarkeitsrelation die natürlichen Zahlen nicht als lineare Kette, sondern in anderer, komplizierterer Art und Weise ordnet:



Wir bemerken, dass sich Zahlen, die in Bezug auf ihre Größe "nahe beieinander" liegen, in Bezug auf die Teilbarkeit als "ziemlich weit voneinander entfernt" erweisen. Anschaulich demonstrieren das die Zahlen 4 und 5 oder 7 und 8.

Wir versuchen nun, von der Betrachtung der Teilbarkeit positiver ganzer Zahlen zur Teilbarkeit der natürlichen Zahlen überzugehen, d. h. die Null in die Betrachtung einzubeziehen. Im Schema würde dadurch ein Kästchen dazu kommen müssen, das höher liegt als alle anderen, da die Null durch jede Zahl teilbar ist, während keine von Null verschiedene Zahl durch Null teilbar ist.
Diesmal bleibt es dem Leser überlassen, die Aussagen 1 bis 7 selbständig zu formulieren und nachzuprüfen.

9. Definition. Jede Relation $\succ$, welche die Bedingungen

1. der Reflexivität ($a \succ a$),
2. der Antisymmetrie (aus $a \succ b$ und $b \succ a$ folgt $a = b$),

3. der Transitivität (aus $a \succ b$ und $b \succ c$ folgt $a \succ c$) erfüllt, heißt Halbordnungsrelation.

Die Halbordnungen spielen dort eine große Rolle, wo keine "echte" lineare Ordnung vorhanden ist, beispielsweise dort, wo jedes Objekt durch mehrere verschiedene, qualitativ nicht vergleichbare Merk- male beschrieben oder bewertet wird.

Als Beispiel dafür könnte man die Bewertung von Ergebnissen verschiedener Sportarten bei einem Wettkampf anführen. Belegt eine Mannschaft in allen Disziplinen bessere Plätze als eine andere, dann ist sofort zu übersehen, dass die erste Mannschaft den größeren Erfolg errang.
Wenn jedoch die besseren Plätze in allen Disziplinen des Programms bis auf eine Ausnahme (sagen wir im Krocketspiel, das aus irgendeinem Grunde diesmal in das Wettkampfprogramm aufgenommen wurde) belegt wurden und sich bei diesem Spiel die zweite Mannschaft als stärker erwies, dann ist die Endplatzierung beider Mannschaften schon nicht mehr so klar.
Ja, die Enthusiasten des Krockets können sogar einen besseren Platz in der Gesamtwertung für die zweite Mannschaft beanspruchen. Auf alle Fälle muss jeder summarischen Verteilung der Plätze eine bestimmte vereinbarte Punktwertung zugrunde liegen.

10. Die Bedingungen 1 bis 3, deren Einhaltung die Relation zu einer Halbordnung macht, sind ziemlich weit gesteckt. Daher können verschiedenartigste Objekte halbgeordnet sein, und das auf ganz verschiedene Arten.
Dementsprechend kann man über eine beliebige Halbordnungsrelation wenig mehr sagen, als dass sie halbgeordnet ist. Insbesondere kann man im allgemeinen auf Objekte, für welche eine Halbordnung definiert ist, die vollständige Induktion nicht anwenden.
Wir wollen nun die Bedingungen 1 bis 3 noch durch die folgenden ergänzen:

4. Wohlordnung.
5. Unbeschränktheit.
6. Jedes vom minimalen Objekt verschiedene Objekt habe einen unmittelbaren Vorgänger.
8. Jedes Objekt habe nur endlich viele Vorgänger.
9. Zu jedem a und $b \succ a$ $(b \neq a)$ existiert ein c, das b unmittelbar vorangeht, derart, dass $c \succ a$ gilt.

Es zeigt sich, dass man aufgrund der Halbordnung der Menge der natürlichen Zahlen durch die den Bedingungen 1 bis 6 und 8 und 9 genügende Relation eine gewisse Modifikation der Methode der vollständigen Induktion vornehmen kann, die in folgendem besteht:

Es sei wieder $A(n)$ eine Aussage, welche sich auf eine willkürlich gewählte Zahl n bezieht. Wir nehmen an, dass folgendes gilt:

a) Die Aussage $A(a)$, in welcher a Minimalzahl im Sinne der Ordnung $\succ$ ist, ist wahr.
b) Ist n eine Zahl und gilt die Aussage $A(m)$ für alle $n > m$ mit $n \neq m$, so gilt auch die Aussage $A(n)$.

Die neue Form des Induktionsprinzips besagt, dass dann, wenn die Bedingungen a) und b) erfüllt sind, die Aussage $A(n)$ für jedes n gilt.

Aufgabe 11. Man leite die "neue" Form des Induktionsprinzips aus seiner "alten" her.

Da die Teilbarkeitsrelation den Bedingungen 1 bis 6, 8 und 9 genügt (man formuliere und verifiziere für die Teilbarkeitsrelation die Bedingungen 8 und 9), ist dieses Induktionsprinzip auf die Teilbarkeitsrelation anwendbar.
Hinsichtlich seiner Verwendung für die Teilbarkeit kann das neue Induktionsprinzip wie folgt formuliert werden:

Ist eine Aussage $A(n)$ gültig für $n = 1$ und folgt aus ihrer Gültigkeit für alle von n verschiedenen Teiler der Zahl n ihre Gültigkeit für die Zahl n, so ist sie für jede Zahl wahr.

11. Wie wir sahen, ist die Division ganzer Zahlen nicht immer ausführbar. Daher ist es zweckmäßig, gleichzeitig mit der Division eine allgemeinere Rechenoperation zu betrachten, die immer ausführbar ist und in den Fällen, in denen die Division ausführbar ist, mit ihr übereinstimmt, nämlich die Division mit Rest.

Definition. Eine Zahl a durch eine Zahl b ($b > 0$) mit Rest teilen heißt die Zahl a in der Form

$$a = bq + r$$

darstellen, wobei $0 \leq r < b$ ist.

Die Zahl q heißt dabei unvollständiger Quotient, die Zahl r der Rest bei Division von a durch b. Offenbar gilt $r = 0$ genau dann, wenn $b|a$ gilt. In diesem Fall ist q gleich dem Quotienten bei Division von a durch b.

Wir werden zeigen, dass die Division mit Rest immer ausführbar ist und dass der unvollständige Quotient und der Rest durch den Dividenden und den Divisor vollständig bestimmt werden, also eindeutig bestimmt sind.
Es sei zunächst $a \geq 0$. Wir schreiben die Zahlen

$$a, a - b, a - 2b, ... \tag{3}$$

so lange nacheinander auf, bis eine negative Zahl auftritt. Früher oder später muss das geschehen (genauer gesagt folgt das aus der Wohlordnung der Menge der natürlichen Zahlen in Bezug auf die Relation $\geq$).
Das letzte der nichtnegativen Glieder der Folge (3), d. h. das kleinste der Glieder, sei die Zahl $a - ba$. Bezeichnen wir sie mit r so erhalten wir

$$a = bq + r \tag{4}$$

Offenbar ist dabei $r < b$, denn sonst wäre die Zahl $r - b$, also $a - (q + 1)b$ nichtnegativ. Das kann aber nicht sein, weil r die kleinste nichtnegative Zahl von (3) sein sollte. Somit ist (4) wirklich die gesuchte Darstellung der Zahl a.

Es sei jetzt $a < 0$. Wir gehen wie oben vor und schreiben die Folge der Zahlen

$$a, a + b, a + 2b, ...$$

auf, bis die erste nichtnegative Zahl r auftaucht (man verifiziert leicht, dass $r < b$ ist). Es sei

$$r = a + bq'$$

Bezeichnen wir $-q'$ mit q, so erhalten wir

$$a = bq + r$$

was zu beweisen war.

Damit ist die Ausführbarkeit der Division mit Rest in allen Fällen bewiesen.

Jetzt beweisen wir die Eindeutigkeit dieser Division: Ist

$$a = bq + r \qquad \text{und zugleich} \qquad a = bq_1 + r_1 \tag{5,6}$$

so folgt $q = q_1$ und $r = r_1$.
Diesen Beweis der Eindeutigkeit darf man keinesfalls dadurch umgehen, dass, man etwa erklärt, die Subtraktion sei eindeutig, daher könne die Folge (3) in eindeutiger Weise konstruiert werden; ihr letztes nichtnegatives Glied sei ebenfalls wohlbestimmt, es werde mit r bezeichnet usw.
Diese Überlegung garantiert uns nicht, dass wir nicht auf ganz anderem Wege andere Werte q und r erhalten könnten.
Vergleichen wir (5) und (6), so folgt

$$bq + r = bq_1 + r_1 \qquad \text{also} \qquad r - r_1 = b(q_1 - q)$$

Daher ist $r - r_1$ durch b teilbar. Nun ist aber $|r - r_1| < b$, und nach Satz 4 ist das nur für $r - r_1 = 0$, d.h. für $r = r_1$ möglich. Dann ist aber

$$b(q - q_1) = 0$$

und da $b \neq 0$ ist, muss $q_1 - q = 0$, also $q_1 = q$ sein. Damit ist die Eindeutigkeit der Division mit Rest bewiesen.
Wir haben somit folgenden Satz hergeleitet:

Satz 7 (Division mit Rest). Zu beliebigen Zahlen a und b ($b > 0$) existieren Zahlen r und q derart, dass $a = bq + r$ und $0 \leq r < b$ ist, wobei die Zahlen r und q eindeutig bestimmt sind.

Aufgabe 12. Man formuliere und beweise den Satz über die Division mit Rest für die geradzahlige Teilbarkeit.

12. Definition. Eine von 1 verschiedene Zahl p wird Primzahl genannt, wenn sie nur durch sich selbst und durch 1 teilbar ist.

Beispielsweise sind die Zahlen 2, 3, 5, 7, 11, 13 usw. Primzahlen.
Eine von 1 verschiedene Zahl, welche keine Primzahl ist, heißt zusammengesetzt.

Satz 8. Es gibt unendlich viele Primzahlen.

Jede Zahl, die gleichzeitig die Zahlen a und b teilt, heißt gemeinsamer Teiler dieser Zahlen. Der größte dieser Teiler von a und b wird größter gemeinsamer Teiler (g.g.T.) genannt und gewöhnlich mit (a, b) bezeichnet. Wenn der g.g.T. der Zahlen a und b gleich 1 ist, werden diese Zahlen zueinander teilerfremd oder relativ prim genannt. Anders ausgedrückt: Zwei Zahlen a, b heißen relativ prim, wenn sie gleichzeitig durch keine Zahl außer 1 teilbar sind.

Satz 9. Sind a und p natürliche Zahlen und ist p eine Primzahl, so gilt entweder $p|a$, oder die Zahlen a und p sind relativ prim.

Jede Zahl, welche gleichzeitig durch die Zahlen a und b teilbar ist, heißt gemeinsames Vielfaches dieser Zahlen. Das kleinste positive dieser Vielfachen von a und b wird kleinstes gemeinsames Vielfaches (k.g.V.) dieser Zahlen genannt.

Satz 10. Ist M ein gemeinsames Vielfaches von a und b und m ihr kleinstes gemeinsames Vielfaches, dann gilt $m|M$.

Satz 11. Das k.g.V. zweier teilerfremder Zahlen ist gleich ihrem Produkt.

Folgerung. Eine Zahl a ist genau dann durch teilerfremde Zahlen b und c teilbar, wenn sie durch deren Produkt teilbar ist.

Satz 12. Gilt $c|ab$ und sind die Zahlen b und c teilerfremd, so gilt $c|a$.

Satz 13. Wenn ein Produkt mehrerer Faktoren durch eine Primzahl p teilbar ist, muss mindestens einer der Faktoren durch p teilbar sein.

Folgerung. Ist p eine Primzahl und $0 < k < p$, so ist die Zahl

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{1 \cdot 2 \cdot ... \cdot (p-1)p}{1 \cdot 2 \cdot ...(k-1)k \cdot 1 \cdot 2 \cdot ...(p-k-1)(p-k)}$$

durch p teilbar.

Satz 14 (Hauptsatz der elementaren Zahlentheorie). Jede von 1 verschiedene positive ganze Zahl kann als Produkt von Primfaktoren dargestellt werden. Diese Darstellung ist eindeutig. (Produkte, die sich nur durch die Reihenfolge ihrer Faktoren unterscheiden, gelten dabei nicht als verschieden.)

Dieser Satz der Zahlentheorie bringt die prinzipielle Möglichkeit zum Ausdruck, jede Zahl in Primfaktoren zu zerlegen. Die praktische Durchführung einer solchen Zerlegung stößt oft auf große Schwierigkeiten, welche auch die moderne Mathematik noch nicht überwinden kann.
Die Zerlegung großer Zahlen in Faktoren oder der Nachweis, dass eine große Zahl Primzahl ist, wird gegenwärtig mit Hilfe elektronischer Rechenautomaten durchgeführt. So wurde erst 1957 gefunden, dass die Zahl $2^{3217} - 1$ eine Primzahl ist. Diese Zahl besteht aus 969 Ziffern und ist die größte bisher bekannte Primzahl. Zum Nachweis, dass es sich tatsächlich um eine Primzahl handelt, brauchte der Rechenautomat $5\frac{1}{2}$ Stunden.

Es sei eine beliebige Zahl a in ein Produkt von Primfaktoren zerlegt. Fassen wir gleiche

Faktoren zusammen, so erhalten wir

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} \tag{r}$$

Wobei $p_1, p_2, ..., p_r$ verschiedene Primzahlen und $\alpha_1, \alpha_2, ..., \alpha_r$ gewisse positive ganze Zahlen sind. Das in der Formel (7) rechts stehende Produkt heißt kanonische Zerlegung der Zahl a.

Satz 15. Zwei Zahlen a und b sind genau dann teilerfremd, wenn kein Primfaktor der kanonischen Zerlegung von a in der kanonischen Zerlegung von b vorkommt.

Satz 16. Ist (7) die kanonische Zerlegung der Zahl a, so ist b genau dann durch a teilbar, wenn die Teilbarkeitsrelationen

$$p_1^{\alpha_1} | b, \quad p_2^{\alpha_2} | b, \quad ..., \quad p_r^{\alpha_r} | b,$$

erfüllt sind.

Aus den Sätzen 15 und 16 folgt, dass die Teilbarkeit einer Zahl durch ein Produkt mehrerer teilerfremder Zahlen damit gleichbedeutend ist, dass diese Zahl durch jede einzelne der Zahlen teilbar ist.

Aufgabe 13. Man schätze den kleinsten Primteiler einer zusammengesetzten Zahl nach oben ab.

Aufgabe 14. Es sei $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ die kanonische Zerlegung einer Zahl a. Dann ist a genau dann durch b teilbar, wenn die kanonische Zerlegung von b die Gestalt

$$b = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$$

hat und $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2$, ..., $0 \leq \beta_r \leq \alpha_r$ gilt.

Aufgabe 15. Man gebe ein Verfahren an, nach dem man aus der kanonischen Zerlegung zweier Zahlen die kanonischen Zerlegungen ihres größten gemeinsamen Teilers und ihres kleinsten gemeinsamen Vielfachen bestimmen kann.

Aufgabe 16. Man beweise: Bezeichnet man die Anzahl der verschiedenen Teiler der Zahl a mit $\tau(a)$ (wobei die 1 und die Zahl a selbst mitgezählt werden) und hat a die kanonische Zerlegung $p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, so gilt

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_r + 1)$$

Aufgabe 17. Man bestimme die Zahl a, wenn bekannt ist, dass sie durch 3 und 4 teilbar und dass $\tau(a) = 14$ ist.

Aufgabe 18. Die kanonische Zerlegung der Zahl a sei $p_1^{\alpha_1} p_2^{\alpha_2}$, und es sei $\tau(a^2) = 81$. Wie groß ist $\tau(a^3)$?

Aufgabe 19. Wie groß ist a, wenn $a = 2\tau(a)$ ist?

Aufgabe 20. Gelten für die geradzahlige Teilbarkeit Sätze, die den Sätzen 11 bis 14 analog sind ?

2 Die Teilbarkeit von Summen und Produkten

1. Bei der Division mit Rest kommt es in vielen Fällen gerade darauf an, den Rest der Division einer Zahl a durch eine Zahl b zu finden, Während die Größe des unvollständigen Quotienten dabei keine Rolle spielt.

Wir wollen zum Beispiel feststellen, auf welchen Wochentag der 1. Januar des Jahres 2000 fällt (natürlich unter der Voraussetzung, dass der gegenwärtig gültige Kalender auch dann noch gültig ist). Ein Blick auf den Kalender zeigt, dass der 1. Januar 1973 ein Montag ist. Die 27 Jahre, die diese beiden Daten von- einander trennen, bestehen aus $27 \cdot 365 + 6$ Tagen (der zweite Summand ist die Anzahl der Tage, welche durch die Anzahl der in diesem Zeitraum liegenden Schaltjahre dazu kommen); also beträgt der gesamte Zeitraum 9861 Tage.
Diese Tage bilden 1408 vollständige Wochen und fünf Tage. Nach Ablauf dieser 1408 Wochen kommt also wieder ein Montag, so dass nach den noch verbleibenden Tagen ein Sonnabend kommen muss, welcher der 1. Januar 2000 ist. Offenbar ist es für die Lösung dieser von uns selbst gestellten Aufgabe völlig unerheblich, wieviel vollständige Wochen in diesen 27 Jahren vergehen.
Entscheidend ist lediglich, wieviel Tage über die Anzahl der vollständigen Wochen hinaus vorhanden sind.

Mit Aufgaben dieser Art werden manchmal vor allem Historiker - besonders die Orientalisten - konfrontiert, wenn sie Daten verschiedener Kalender miteinander vergleichen sollen.
Es hat den Anschein, als würde man den Rest bei Division einer Zahl durch eine andere am leichtesten erhalten, indem man die Division tatsächlich ausführt. Bei der praktischen Durchführung einer solchen Division stellt man jedoch recht oft fest, wie umständlich ein solches Verfahren vor allem dann ist, wenn der betreffende Dividend nicht in unserem vertrauten Dezimalsystem, sondern als komplizierter Ausdruck, etwa in der Form $2^{1000} + 3^{1000}$ gegeben ist.

Außerdem beansprucht gerade die Berechnung des unvollständigen Quotienten den Löwenanteil der Arbeit, obwohl uns dieser an und. für sich gar nicht interessiert. Deshalb ist es notwendig, Verfahren zu entwickeln, mit deren Hilfe man den Rest unmittelbar erhält, ohne erst den unvollständigen Quotienten berechnen zu müssen.

Wir führen ein solches Verfahren an Hand des oben dargestellten Beispiels vor. Dabei überlegen wir folgendermaßen: Jedes Jahr, das kein Schaltjahr ist, besteht aus 365 Tagen, hat also 52 ganze Wochen und einen Tag.
Ein Schaltjahr dagegen hat ebenso viele ganze Wochen und zwei Tage. Das heißt, der Zeitraum vom 1. Januar 1973 bis zum 1. Januar 2000 enthält eine gewisse Anzahl (es ist völlig unwichtig zu wissen wieviel) ganzer Wochen plus eine Anzahl von Tagen, die gleich der Zahl der Jahre dieses Zeitraumes ist, wobei für die Schaltjahre jeweils ein zusätzlicher Tag hinzukommt.

Diese Anzahl der Tage ist $27 + 6 = 33$. Ziehen wir davon wieder die Anzahl der Tage für ganze Wochen ab, so erhalten wir noch fünf übrig bleibende Tage, die wir zu unserem

Montag dazu zählen. Es zeigt sich, dass ein solches "Ersetzen eines Jahres durch einen Tag" das Modell eines äußerst allgemeinen Verfahrens ist, mit welchem wir uns im folgenden beschäftigen wollen.

2. Definition. Wir nennen die Zahlen a und b restgleich hinsichtlich der Division durch m, wenn die Reste bei Division von a und b durch m einander gleich sind.

Wir wollen einige Eigenschaften restgleicher Zahlen ermitteln.

Satz 17. Die Zahlen a und b sind dann und nur dann restgleich hinsichtlich der Division durch m, wenn ihre Differenz $a - b$ durch m teilbar ist.

Satz 18. Sind die Zahlen $a_1, a_2, ..., a_n$ den Zahlen $b_1, b_2, ..., b_n$ hinsichtlich der Division durch m restgleich, so sind es auch die Summen $a_1 + a_2 + ... + a_n$ und $b_1 + b_2 + ... + b_n$ sowie die Produkte $a_1 a_2 ... a_n$ und $b_1 b_2 ... b_n$.

Folgerung. Sind die Zahlen a und b hinsichtlich der Division durch m restgleich, so sind es auch die Zahlen a^n und b^n für jedes natürliche n.

Der Satz 18 und seine Folgerung liefern schon viele Möglichkeiten, Reste bei Division zu erhalten. Wir führen einige Beispiele an.

Beispiel 1. Man bestimme den Rest bei Division der Zahl $A = 13^{16} - 2^{25} \cdot 5^{15}$ durch 3.

Offenbar sind hinsichtlich der Division durch 3 die 13 mit der 1, die 2 mit der -1 und die 5 ebenfalls mit der -1 restgleich. Aufgrund des bisher Bewiesenen heißt das:
Die Zahl A ist hinsichtlich der Division durch die Zahl 3 restgleich mit der Zahl $1^{16} - (-1)^{25} - (-1)^{15} = 1 - 1 = 0$. Das heißt, der gesuchte Rest ist Null und A demzufolge durch 3 teilbar.

Beispiel 2. Man bestimme den Rest bei Division derselben Zahl A durch 37.

Dazu stellen wir die Zahl A in folgender Form dar:

$$A = (13^2)^3 - (2^5)^5 \cdot (5^3)^5$$

Bei Division durch 37 ist $13^2 = 169$ restgleich mit -16, ferner $2^5 = 32$ restgleich mit -5 und $5^3 = 125$ restgleich mit 14. Somit ist die gesamte Zahl A restgleich mit

$$(-16)^8 - (-5)^5 \cdot (+14)^5$$

oder, was das gleiche ist, mit $(16^2)^4 + 70^5$. Da $16^2 = 256$ restgleich mit -3 und 70 restgleich mit -4 ist, heißt das, A ist restgleich mit $-(-3)^4 + (-4)^5$ oder, was das gleiche ist, mit $81 - (25)^2$, also mit

$$81 - (-5)^2 = 81 - 25 = 56$$

Schließlich ist 56 hinsichtlich der Division durch 37 restgleich mit 19; diese Zahl ist nicht negativ und kleiner als 37, also der gesuchte Rest.

Aufgabe 21. Man bestimme den Rest bei Division von

a) $A = (116 + 17^{17})^{21}$ durch 8;
b) $A = 14^{256}$ durch 17.

Aufgabe 22. Man beweise, dass für jedes n die folgenden Teilbarkeitsbeziehungen gelten:
a) $6|(n^3 + 11n)$;
b) $9|(4^n + 15n - 1)$;
c) $3^{n+2}|(10^{3^n} - 1)$;
d) $(a^2 - a + 1)|(a^{2n+1} + (a-1)^{n+2})$ für beliebiges a.

3. Die hinsichtlich der Division durch m restgleichen Zahlen a und b werden auch kongruent modulo m genannt, in Zeichen:

$$a \equiv b \pmod{m} \tag{4}$$

Diese Formel selbst nennt man eine Kongruenz, die natürliche Zahl m den Modul.

Die Kongruenz zweier ganzer Zahlen nach einem festgelegten Modul m oder, was das gleiche ist, ihre Restgleichheit hinsichtlich der Division durch m ist ebenfalls eine Relation, welche zwei ganze Zahlen miteinander verknüpft. Einige Eigenschaften dieser Kongruenzrelation nach einem Modul seien hier aufgeführt:

1. Reflexivität: $a \equiv a \pmod{m}$, denn $a - a = 0$ ist durch m teilbar.

2. Symmetrie: Ist $a \equiv b \pmod{m}$, dann ist auch $b \equiv a \pmod{m}$.
Ist nämlich $a - b$ durch m teilbar, so ist es nach Satz 5 auch $b - a$.

3. Transitivität: Ist $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$, so gilt $a \equiv c \pmod{m}$.
Zum Beweis genügt es zu bemerken, dass aus $m|(a - b)$ und $m|(b - c)$ nach Satz 6 die Beziehung $m|(a - c)$ folgt.

Wenn eine Relation (wir wollen sie mit $\sim$ bezeichnen) die Eigenschaften der Reflexivität, der Symmetrie und der Transitivität besitzt, wird sie eine Äquivalenzrelation genannt. Das einfachste Beispiel einer Äquivalenzrelation über einer Menge von Zahlen ist die Gleichheitsrelation.

Aufgabe 23. Eine Äquivalenzrelation $\sim$ über einer Menge von Zahlen zerlegt diese Menge so in Klassen (sogenannte Äquivalenzklassen), dass je zwei Zahlen aus ein und derselben Klasse durch die Äquivalenzrelation verknüpft sind, jedoch keine zwei Zahlen aus verschiedenen Klassen (der Leser möge das beweisen). In dieser Aufgabe ist von einer Äquivalenzrelation die Rede, durch welche Zahlen verknüpft werden.

Das ist jedoch unwesentlich, die Aussage der Aufgabe gilt für Äquivalenzrelationen, welche Objekte ganz willkürlicher Art verknüpfen. Da die Kongruenzbeziehung nach einem Modul m eine Äquivalenzrelation ist, zerlegt auch sie die Menge der ganzen Zahlen in Klassen. Diese Klassen nennt man Restklassen modulo m.

4. Die Anzahl der Restklassen modulo m ist gleich m. Zwei Zahlen gehören nämlich dann und nur dann ein und derselben Restklasse modulo m an, wenn sie bei der Division durch m ein und denselben Rest liefern. Als Reste bei der Division durch m können aber nur die m verschiedenen Werte $0, 1, ..., m - 1$ auftreten. Daraus folgt, dass die

Anzahl der Klassen gleich m ist.

Wir weisen auf einen außerordentlich interessanten Umstand hin:
Eine Restklasse modulo m_1 ist genau dann in einer Restklasse modulo m_2 enthalten, wenn $m_2|m_1$ gilt.

Zum Beweis betrachten wir die Restklasse K_1 modulo m_1, welche die Zahl 0 enthält. Offenbar besteht K_1 aus allen Zahlen, die bei Division durch m_1 den Rest 0 liefern, d. h., die durch m_1 teilbar sind.
Insbesondere enthält K_1 die Zahl m_1.
Eine Restklasse modulo m_2, die K_1 enthält, enthält ebenfalls die Null und besteht deshalb aus allen Zahlen, die durch m_2 teilbar sind. Da darin die Zahl m_1 enthalten ist, muss $m_2|m_1$ gelten. Damit ist die Notwendigkeit bewiesen; die Hinlänglichkeit ist offensichtlich.

Auf diese Weise kann eine Teilbarkeitsrelation durch eine Beziehung zwischen Restklassen definiert werden. Dieses Verfahren erlaubt es, für Objekte weitaus allgemeinerer und komplizierterer Natur, als es die natürlichen Zahlen sind, eine Teilbarkeit zu definieren. Die folgerichtige Entwicklung dieser Gedanken führte zur Gruppentheorie, einem wichtigen Zweig der modernen Algebra, der in der theoretischen Physik und in der Kristallographie Anwendung findet.

Nun wollen wir die Aufzählung der Eigenschaften der Kongruenz von Zahlen fortsetzen. Aus Satz 18 folgt unmittelbar:.

5. Ist $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$, so ist $a + c \equiv b + d \pmod{m}$.

Folgerung. Ist $a \equiv b \pmod{m}$, so ist $a + r \equiv b + r \pmod{m}$ für jedes ganze r.

6. Ist $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$, so ist $a \cdot c \equiv b \cdot d \pmod{m}$.

Die Eigenschaften 5 und 6 zeigen, dass man Kongruenzen ähnlich wie Gleichheiten seitenweise addieren und multiplizieren kann.

Aufgabe 24. Ist über der Menge der ganzen Zahlen eine Äquivalenzrelation gegeben, die diese Menge so in m Klassen einteilt, dass aus $a \sim b$ und $c \sim d$ die Äquivalenz $a + c \sim b + d$ folgt, so ist diese Relation eine Kongruenz nach dem Modul m (d. h., es gilt $a \sim b$ dann und nur dann, wenn $a \equiv b \pmod{m}$ ist).

Aufgabe 25. Man formuliere und beweise die Regeln für das Kürzen von Kongruenzen.

Aufgabe 26. Ist p eine Primzahl und a nicht durch p teilbar, so sind keine zwei Zahlen aus der Folge $a, 2a, 3a, ..., (p-1)a$ kongruent modulo p. Dabei ergeben sich bei Division der Zahlen $a, 2a, 3a, ..., (p-1)a$ alle Reste außer der Null je einmal.

Aufgabe 27 (Satz von Wilson). Eine Zahl p ist genau dann Primzahl, wenn

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

durch p teilbar ist.

Aufgabe 28. Man formuliere und beweise für die Restgleichheit einen Satz, der dem Satz 16 analog ist.

3 Restgleichheits- und Teilbarkeitskriterien

1. Eine ganz allgemeine Methode, bei Division einer willkürlichen, aber festen natürlichen Zahl a durch eine gegebene Zahl m den Rest zu finden, besteht in folgendem: Wir konstruieren eine Folge natürlicher Zahlen, welche in Bezug auf die Division durch m restgleich sind:

$$a = A_0, A_1, A_2, ... \tag{8}$$

Das Verfahren zur Bildung der Folge (8) wählen wir so, dass nach jedem Glied, welches größer oder gleich m ist, noch mindestens ein weiteres Glied folgt. Dann ist offensichtlich das letzte Glied der Folge (8) in Bezug auf die Division von a durch m (falls ein solches existiert) gleich dem Rest r bei Division von a durch m.

Das einfachste Beispiel einer solchen Folge ist die Folge (3) aus § 1, Abschnitt 11.

Dem Wesen nach lassen sich Aufgaben zur Bestimmung des Bestes in den Beispielen 1 und 2 des vorigen Paragraphen auf die Bildung einer Folge dieses Typs zurückführen.
Jede Methode zur Bildung einer Folge (8) nennen wir ein Kriterium für Restgleichheit hinsichtlich der Division durch m.
Insbesondere ist eines der Kriterien für Restgleichheit hinsichtlich der Division durch m das Verfahren aufeinanderfolgender Subtraktionen, bis man zum ersten mal eine Zahl erhält, die kleiner ist als an.

2. Offenbar muss ein Kriterium für Restgleichheit folgenden drei Forderungen genügen, damit man davon überzeugt sein kann, dass es reibungslos funktioniert:

1. Es muss wohlbestimmt sein, d. h., die Zahl a muss alle Glieder der Folge (8) vollständig festlegen und darf keine Willkür zulassen.

2. Es muss allgemeingültig, d. h. auf jede natürliche Zahl a anwendbar sein.

3. Schließlich muss garantiert sein, dass in der Folge (8) mindestens ein Glied kleiner als m ist. Diese Forderung ist gleichbedeutend damit, dass die Folge (8) nur aus endlich vielen Gliedern bestehen darf und dass das Verfahren zur Bildung der Folge nicht unbeschränkt fortgesetzt werden kann, sondern früher oder später durch das Auftreten des Restes von a bei Division durch m beendet wird. Ein Kriterium für Restgleichheit muss also zum Ziel führen.

Die genannten Forderungen können auf ganz verschiedenen Wegen erreicht werden. Der natürlichste Weg besteht darin, dass wir versuchen, eine Funktion $f(x)$ zu finden, welche folgende Bedingungen erfüllt:

a) $f(x)$ ist für $x \geq m$ eine natürliche Zahl;
b) $f(x)$ ist für $x < m$ nicht definiert (hat keinen Sinn);

(Es ist durchaus nicht ungewöhnlich, dass die eine oder andere Funktion für einige

Werte ihres Arguments nicht definiert ist. So ist zum Beispiel der Wert der Funktion $\frac{1}{x(x-1)}$ weder für $x = 0$ noch für $x = 1$ definiert.)

c) wenn $f(x)$ definiert ist, so ist $f(x) < x$;
d) wenn $f(x)$ definiert ist, so sind die Zahlen x und $f(x)$ restgleich hinsichtlich der Division durch m.

Solche Funktionen existieren. Ein Beispiel dafür ist die Funktion

$$f_0(x) = \begin{cases} x - m & \text{für } x \geq m \\ \text{nicht definiert} & \text{für } x < m \end{cases}$$

Gerade diese Funktion vermittelt die Bildung der Folge (3) in § 1.

Jeder Funktion $f(x)$, die den Bedingungen a) bis d) genügt, entspricht eine Methode zur Bildung der Folge (8), d. h. ein Kriterium der Restgleichheit hinsichtlich der Division durch m.
Um das zu zeigen, nehmen wir eine beliebige natürliche Zahl a und bilden mit ihr die Folge der Zahlen

$$A_0, A_1, A_2, ... \tag{9}$$

wobei $A_0 = a$ und $A_{k+1} = f(A_k)$ für $k = 0, 1, 2, ...$ ist. Für $A_k \geq m$ ist der Wert der Funktion $f(A_k)$ definiert; daher folgt auf A_k mindestens ein Glied.
Ist aber $A_k < m$, so ist $f(A_k)$ nicht definiert, und A_k ist das letzte Glied der Folge (9). Damit haben wir tatsächlich ein Kriterium für Restgleichheit erhalten.

3. Nun zeigen wir, dass dieses Kriterium den Forderungen 1, 2 und 3 genügt.
Die erste Forderung ist erfüllt, weil jedes Glied der Folge (9) das nachfolgende Glied eindeutig bestimmt (natürlich nur, wenn es ein solches tatsächlich gibt).

Dabei tritt jedoch ein subtiles Problem auf, das zwar nicht augenfällig, aber außerordentlich Wichtig ist. Es besteht darin, dass man beim Aufstellen der Folge (9) noch vor der Berechnung des Wertes $f(A_k)$ ergründen muss, ob dieser Wert überhaupt existiert. Mit anderen Worten, wir müssen feststellen, ob die Zahl A_k größer oder kleiner als m ist. Sind die Zahlen A_k und m in einer für diesen Vergleich geeigneten Form gegeben, etwa in Dezimalschreibweise, so lassen sie sich mühelos vergleichen.
Ein Größenvergleich etwa der Zahlen $2^{20} - 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$ und $3^{10} - 78 \cdot 757$ erfordert jedoch eine umfangreichere Arbeit, obwohl die erste Zahl gleich 1 und die zweite gleich 3 ist.

Im Zusammenhang damit werden wir im folgenden das Kriterium für Restgleichheit ausschließlich auf positive Zahlen in Dezimaldarstellung anwenden.

Hinsichtlich der zweiten Forderung genügt folgende Feststellung: Ist $a \geq m$, dann können wir faktisch mit der Bildung der Folge beginnen, nachdem wir den Wert $f(a)$ berechnet haben, welcher nach Voraussetzung existiert. Ist $a < m$, so ist $f(a)$ nicht definiert. In diesem Fall ist a selbst Rest hinsichtlich der Division durch an. Dann besteht eben die ganze Folge (9) nur aus der Zahl a, also aus einem einzigen Glied.

Wir kommen nun zur dritten Forderung. Nach Voraussetzung ist die Funktion $f(x)$ so

ausgewählt, dass alle Glieder der Folge (9) ein und dasselbe Vorzeichen haben, während ihre absoluten Beträge abnehmen.
Da das erste Glied der Folge positiv ist, gibt es in ihr ein kleinstes nichtnegatives Glied. (Man prüft leicht nach, dass dieses Glied in der Folge eine Nummer hat, die höchstens gleich a ist.)

Wäre dieses Glied (wir bezeichnen es mit α) größer oder zumindest gleich m (also nicht kleiner als m), so würde der Wert $f(\alpha)$ existieren und ebenfalls nichtnegativ und kleiner als α sein.
Das heißt aber, das Glied α wäre nicht das letzte unter den Gliedern der Folge (9). Demnach muss das letzte nichtnegative Glied der Folge (9) kleiner als m sein. Dann ist aber der Wert $f(\alpha)$ nicht definiert, und α ist überhaupt das letzte Glied der Folge. Somit ist der Bildungsprozess der Folge beendet, und ihr letztes Glied ist der Rest von a bei Division durch m.

Damit haben wir festgestellt, dass das von uns beschriebene Kriterium der Restgleichheit tatsächlich die geforderten Eigenschaften hat, also wohlbestimmt und allgemeingültig ist und zum Ziel führt.
Verfahren, welche diese drei Eigenschaften besitzen, werden Algorithmen genannt. Sie beginnen in der modernen Mathematik eine immer größere Rolle zu spielen. Einige einfache Beispiele für Algorithmen wurden am Ende des Abschnitts 1 in § 1 angeführt. Andere Beispiele werden wir im folgenden kennenlernen.

4. Einer der wichtigsten Algorithmen in der Mathematik ist der sogenannte Euklidische Algorithmus:

Es seien a und b zwei natürliche Zahlen, $0 < b < a$. Wir dividieren a durch b mit Rest:

$$a = bq_0 + r_1, \qquad \text{wobei } 0 \leq r_1 < b$$

ist. Ist $r_1 \neq 0$, dann kann b durch r_1 mit Rest dividiert werden, und es ergibt sich

$$b = r_1 q_1 + r_2, \qquad \text{wobei } 0 \leq r_2 < r_1$$

ist.
Wenn wir dieses Verfahren, jeweils den Divisor bei einer Division mit Rest durch den Rest zu dividieren, fortsetzen, erhalten wir die weiteren Gleichungen

$$r_1 = r_2 q_2 + r_3$$
$$r_2 = r_3 q_3 + r_4 \qquad \ldots$$

Wir beweisen nun, dass das hier beschriebene Verfahren wirklich ein Algorithmus ist, d. h. wohlbestimmt und allgemeingültig ist und zum Ziel führt.

Wir bemerken, dass das betrachtete Verfahren darin besteht, nacheinander Divisionen mit Rest durchzuführen. Deshalb ergeben sich Wohlbestimmtheit sind Allgemeingültigkeit dieses Verfahrens aus der uneingeschränkten Ausführbarkeit und der Eindeutigkeit der Division mit Rest.

Dass das Verfahren zu einem Ziel führt, lässt sich ebenfalls relativ einfach zeigen. Die Zahl b und die Divisionsreste bilden offenbar eine abnehmende Folge nichtnegativer Zahlen

$$b, r_1, r_2, ... \tag{10}$$

Die Anzahl aller nichtnegativen Glieder, die nicht größer sind als b, ist aber $b+1$. Daher kann auch die Folge (10) nicht mehr als b Glieder enthalten, so dass unser Verfahren aus höchstens b Divisionen mit Rest bestehen kann.[2] Somit ist das betrachtete Verfahren tatsächlich ein Algorithmus und trägt seinen Namen völlig zu Recht.

Wir werden nun die Bedingungen klären, unter denen dieses Verfahren abbricht. Offenbar muss die letzte Division so beschaffen sein, dass keine weitere Division durch den verbleibenden Rest mehr möglich ist. Das trifft aber nur dann zu, wenn dieser letzte Rest Null ist, d.h., wenn die letzte Division aufgeht.

Aufgabe 29. Man beweise:
a) Der letzte von Null verschiedene Rest r_m des Euklidischen Algorithmus für zwei Zahlen a und b ist der größte gemeinsame Teiler (a, b) von a und b.

b) Zu je zwei natürlichen Zahlen a und b gibt es ganze Zahlen A und B derart, dass $aA + bB = (a, b)$ ist.

Aufgabe 30. Man folgere aus der Aussage b) der Aufgabe 29 die Sätze 9, 12, 13 und 14. (Es sei betont, dass sich unsere Überlegungen zum Euklidischen Algorithmus nur auf die Existenz der Division mit Rest gründeten. Wir haben dabei weder die Sätze 9 bis 14 noch irgendwelche anderen Überlegungen benutzt, die auf dem Hauptsatz der elementaren Zahlentheorie (Eindeutigkeit der Primzahlzerlegung) beruhen.)

5. Natürlich ist die in Abschnitt 3 angegebene Beschreibung des Begriffs Algorithmus nicht etwa dessen genaue Definition; diese ist verhältnismäßig kompliziert und. kann deshalb hier nicht formuliert werden.
Allerdings werden durch die dort aufgeführten Forderungen diejenigen Bedingungen ziemlich genau widergespiegelt, denen mathematische Verfahren genügen müssen, damit sie als Algorithmen bezeichnet werden können. Die Bedeutung der Algorithmen wird dadurch bestimmt, dass sie einheitliche Methoden zum Lösen einer ganzen Reihe von Aufgaben gleichen Typs liefern. Die Algorithmen, von denen oben die Rede ist, ermöglichen es, den Rest einer Zahl 0 bei Division durch eine feste Zahl m zu berechnen.

Spezialfälle von Algorithmen sind die verschiedensten Berechnungen mit Hilfe von Formeln, in denen statt der Buchstaben Zahlen eingesetzt werden können.
Man könnte etwa sagen, alle mathematischen Probleme, deren Lösung automatisiert werden kann, lassen sich auf Algorithmen zurückführen. Dabei ist es kein Zufall, dass die Entwicklung der Algorithmentheorie historisch mit der Entstehung und verbreiteten Anwendung von Rechenmaschinen zusammenfällt.

Auf Algorithmen lassen sich nicht nur Rechenaufgaben im engeren Sinne zurückführen,

[2] In Wirklichkeit ist die Anzahl dieser Divisionen höchstens gleich $5 \log b$, wie man mit Hilfe der Fibonaccischen Zahlen erkennt. Der Leser vergleiche dazu das ebenfalls in dieser Reihe erschienene Bändchen von N. N. Worobjow, Die Fibonaccischen Zahlen.

d. h. solche Aufgaben, in denen man nach mehr oder weniger komplizierten Regeln auf der Grundlage von Ausgangsgrößen ein Resultat in Zahlen erhalten kann.
Man kann auch die Aufgabe stellen, einen geeigneten Algorithmus zu bestimmen, der es gestattet, jedes Problem eines bestimmten Teilgebiets der Mathematik zu lösen. Ein solcher Algorithmus muss aus den Formulierungen der Sätze die Beweise dafür herleiten können. Wie phantastisch das auch klingen mag, solche Algorithmen existieren tatsächlich, allerdings nicht für sehr breite Gebiete der Mathematik. Es gibt aber auch einige Gebiete (beispielsweise alle diejenigen, welche die ganze Arithmetik umfassen), für die es prinzipiell keine solchen Algorithmen geben kann.

6. Wir wollen nun unter Benutzung der in Abschnitt 1 dargestellten Verfahren zur Konstruktion Von Kriterien für Restgleichheit einige solcher Kriterien aufstellen. Hier und auch im folgenden nehmen wir an, dass die Zahlen, deren Divisionsreste wir suchen, im Dezimalsystem dargestellt sind.
Als erstes suchen wir ein Kriterium für Restgleichheit bei Division durch 5.

Es sei A eine natürliche Zahl, die wir in der Form $10a + b$ darstellen wollen (b ist die letzte Ziffer der Zahl A). Wir setzen

$$f_1(A) = \begin{cases} b & \text{für } A \geq 10 \\ b - 5 & \text{für } 5 \leq A < 10 \\ \text{nicht definiert} & \text{für } A < 5 \end{cases}$$

Der Leser möge selbst nachprüfen, dass die so definierte Funktion den Bedingungen a) bis d) aus Abschnitt 2 genügt.

Somit genügt es zum Berechnen des Bestes einer Zahl bei Divisionen durch 5, die letzte Ziffer dieser Zahl zu betrachten. Ist diese Ziffer kleiner als 5, so ist sie selbst der gesuchte Rest; andernfalls muss 5 von der letzten Ziffer subtrahiert werden.
Wir erkennen, dass die Anwendung des Kriteriums für Restgleichheit auf eine beliebige Zahl auf die Bildung einer Folge des Typs (9) führt, Welche aus höchstens drei Gliedern besteht.

Selbstverständlich besteht das Ziel aller dieser Überlegungen nicht darin, das wohlbekannte "Teilbarkeitskriterium" für 5 zu entdecken, sondern vielmehr darin, es durch das (in Abschnitt 2 beschriebene) einheitliche Verfahren zu erhalten.

Aufgabe 31. Man gebe entsprechende Kriterien für Restgleichheit bei Division durch 2, 4, 8, 10, 16, 20 und 25 an und analysiere sie.

Aufgabe 32. Wir schreiben die natürliche Zahl A in der Form

$$10^k a + b \qquad (0 \leq b < 10^k)$$

und setzen

$$f(A) = \begin{cases} b & \text{für } A \geq 10^k \\ \text{Rest von } A \text{ bei Division durch } m & \text{für } m \leq A < 10^k \\ \text{nicht definiert} & \text{für } A < m \end{cases}$$

Für welche Zahlen m ist dieser Algorithmus bei bestimmtem k ein Kriterium für Restgleichheit?

17. Als zweites Beispiel untersuchen wir das Kriterium für Restgleichheit bei Division durch 3. Dazu schreiben wir die natürliche Zahl A in der Form

$$10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$$

wobei $0 \leq a_i < 10$ ist (die Zahlen $a_0, a_1, ..., a_{n-1}, a_n$ sind die Ziffern der Zahl A). Wir setzen

$$f_2(A) = \begin{cases} a_0 + a_1 + ... + a_{n-1} + a_n & \text{für } A \geq 10 \\ \text{Rest bei Division durch } 3 & \text{für } 3 \leq A < 10 \\ \text{nicht definiert} & \text{für } A < 3 \end{cases}$$

Aufgabe 33. Man beweise, dass die Funktion $f_2(x)$ den Bedingungen a) bis d) aus Abschnitt 2 genügt und damit ein Kriterium für Restgleichheit bei Division durch 3 definiert.

Aufgabe 34. Man wende dieses Kriterium für Restgleichheit bei Division durch 3 auf folgende Zahlen an:

a) 858773 und 789988;
b) auf die Zahl, die in Dezimalschreibweise aus 4444 Vieren besteht.

Aufgabe 35. Man bestimme und untersuche ähnliche Kriterien für Restgleichheit bei Division durch 7, 9, 11, 13 und 37.

8. Bei vielen Divisionsaufgaben ist sowohl die Größe des unvollständigen Quotienten als auch die Größe des Divisionsrestes unwesentlich; von Interesse für uns ist nur, ob der Rest Null ist oder nicht, ob also die erste Zahl durch die zweite teilbar ist oder nicht. Nach dem in Abschnitt 1 Gesagten ist klar, wie Aufgaben solcher Art zu behandeln sind.

Wir nennen Zahlen a und b teilbarkeitsgleich hinsichtlich der Division durch m, wenn entweder sowohl a als auch b durch m teilbar ist oder wenn weder a noch b durch m teilbar ist.

Aufgabe 36. Für beliebiges m sind je zwei hinsichtlich der Division durch m restgleiche Zahlen auch teilbarkeitsgleich in Bezug auf m. Man beweise, dass die Umkehrung falsch ist.

Aufgabe 37. Für welche m folgt aus der Teilbarkeitsgleichheit zweier Zahlen hinsichtlich der Division durch m ihre Restgleichheit in Bezug auf m?

Aufgabe 38. Man beweise, dass die Beziehung der Teilbarkeitsgleichheit hinsichtlich einer gegebenen Zahl m eine Äquivalenzrelation ist und die Menge der ganzen Zahlen in zwei Klassen zerlegt.

Aufgabe 39. Gilt Satz 18 für teilbarkeitsgleiche Zahlen? Gilt auch die Folgerung?

9. Angenommen, wir sollten feststellen, ob die Zahl A durch m teilbar ist. Wir bilden

eine Folge ganzer Zahlen

$$A = A_0, A_1, A_2, ... \tag{11}$$

die dem absoluten Betrag nach abnehmen und mit A hinsichtlich der Division mit Rest durch m teilbarkeitsgleich sind. Die Bildung der Folge (11) nehmen wir so vor, dass auf jedes Glied dieser Folge, das absolut mindestens gleich m ist, noch wenigstens ein Glied folgt. Wird dabei das letzte Glied von (11) gleich Null, dann ist A durch m teilbar, ist das letzte Glied von Null verschieden, dann ist A nicht durch m teilbar.

Jedes Verfahren zur Bildung einer Folge (11) nennen wir ein Kriterium für Teilbarkeit durch m.

Aufgabe 40. Man beweise, dass jedes Kriterium für Restgleichheit hinsichtlich der Division durch m ein Kriterium für Teilbarkeit durch m ist.

Offenbar müssen Teilbarkeitskriterien den gleichen Bedingungen wie Kriterien für Restgleichheit genügen: wohlbestimmt und allgemeingültig sein und zum Ziel führen.
Man prüft leicht nach (der Leser sollte es tun), dass mit Hilfe jeder Funktion $f(x)$, die den Bedingungen a) bis d) aus Abschnitt 2 und zusätzlich der Bedingung

d*) wenn $f(x)$ definiert ist, sind die Zahlen m und $f(x)$ teilbarkeitsgleich hinsichtlich der Division durch m

genügt, ein Teilbarkeitskriterium für m auf die gleiche Art und Weise gebildet werden kann wie das Kriterium für Restgleichheit hinsichtlich der Division durch m mit Hilfe jeder Funktion, welche den Bedingungen a) bis d) genügt.

Wir gehen nun einige Teilbarkeitskriterien an.
Nach Satz 16 genügt es, die Teilbarkeit von Zahlen durch Zahlen der Form p^α (Primzahlpotenzen) festzustellen.

10. Kriterium für Teilbarkeit durch 7. Es sei A eine natürliche Zahl. Wie früher schreiben wir A in der Form

$$10a + b \qquad \text{mit } 0 \leq b < 10$$

Wir setzen

$$f_3(A) = \begin{cases} a - 2b & \text{für } A \geq 19 \\ \text{Rest bei Division von } A \text{ durch } 7 & \text{für } 7 \leq A < 19 \\ \text{nicht definiert} & \text{für } A < 7 \end{cases}$$

Aufgabe 41. Man weise nach, dass die Funktion $f_3(A)$ den Bedingungen a) bis c) und d*) genügt.

Die Funktion $f_3(A)$ liefert uns das bekannte Teilbarkeitskriterium für 7: Die Zahl $10a+b$ $(0 \leq b < 10)$ ist dann und nur dann durch 7 teilbar, wenn die Zahl $a - 2b$ durch 7 teilbar ist. Diese Zahl wird mit Hilfe der gleichen Methode auf ihre Teilbarkeit durch 7 überprüft usw.

Aufgabe 42. Man beweise, dass das erhaltene Kriterium für Teilbarkeit durch 7 kein Kriterium für Restgleichheit hinsichtlich der Division durch 7 mit Rest ist.

11. Kriterium für Teilbarkeit durch 13. Wir schreiben die natürliche Zahl A in der Form

$$10a + b \qquad \text{mit } 0 \leq b < 10$$

und setzen

$$f_4(A) = \begin{cases} a + 4b & \text{für } A \geq 40 \\ \text{Rest bei Division von } A \text{ durch } 13 & \text{für } 13 \leq A < 40 \\ \text{nicht definiert} & \text{für } A < 13 \end{cases}$$

Aufgabe 43. Man weise nach, dass die Funktion $f_4(A)$ den Bedingungen a) bis c) und d*) genügt, und formuliere das erhaltene Kriterium für Teilbarkeit durch 13.

Aufgabe 44. Welche Auswirkungen hat es, wenn man in der Definition der Funktion f_4 die Zahl 40 durch eine kleinere ersetzt ?

Aufgabe 45. Man gebe Kriterien für Teilbarkeit durch 17, 19, 23, 29 und 31 an, die denjenigen für Teilbarkeit durch 7 und 13 ähnlich sind.

Aufgabe 46. Man formuliere zwei Kriterien für Teilbarkeit durch 49.

12. In den vorangegangenen Abschnitten dieses Paragraphen lernten wir eine große Zahl verschiedenartigster Kriterien für Restgleichheit und für Teilbarkeit kennen. Das praktische Ziel bei der Konstruktion aller dieser Kriterien besteht darin, bequeme Algorithmen zum Auffinden der Reste hinsichtlich der Division durch bestimmte Zahlen (Kriterien für Restgleichheit) zu erhalten bzw. Algorithmen, mit deren Hilfe wir erkennen, ob diese Reste gleich Null sind oder nicht (Teilbarkeitskriterien).
Inwiefern haben wir nun dieses Ziel erreicht?

Einige Kriterien für Restgleichheit, wie zum Beispiel bei Division durch 2, 3, 5, 10, erwiesen sich tatsächlich als höchst praktisch und bequem. Die Anwendung anderer Kriterien wiederum ist mit mehr oder weniger aufwendigen Rechnungen verbunden.
Naturgemäß sucht man also nach solchen Kriterien für Teilbarkeit und Restgleichheit, deren Anwendung auf möglichst einfachem Weg zum Ziel führt.

Eine dieser Schwierigkeiten, auf die wir hier stoßen, besteht darin, dass wir lernen müssen, die Einfachheit (bzw. die Kompliziertheit) der Anwendung des einen oder anderen Kriteriums durch eine Zahl zu bewerten. Als eine solche charakteristische Zahl könnte man beispielsweise die Anzahl der Rechenoperationen mit einstelligen Zahlen nehmen, welche bei Anwendung des betreffenden Kriteriums ausgeführt werden müssen.
Leider hängt jede dieser Charakteristiken für das Ausmaß der notwendigen Rechnungen in starkem Maße von den individuellen Eigenschaften der Zahl ab, deren Teilbarkeit wir untersuchen wollen.

So ist zum Beispiel leicht zu erkennen, dass der Rest von 31025 bei Division durch 8 die Zahl 1 ist. Dazu genügt es, den Rest von 25 bei Division durch 8 zu bilden. Sollen wir aber den Rest von 30525 bei Division durch 8 finden, so müssen wir die Zahl 525 durch 8 mit Rest dividieren, und das erfordert schon eine größere Anzahl von Rechenoperationen (gleichgültig, ob sie im Kopf oder schriftlich durchgeführt werden).

Als weiteres Beispiel wollen wir das Kriterium für Restgleichheit hinsichtlich der Division durch 37 untersuchen (vgl. Aufgabe 35). Der Rest von 11014023 bei Division durch 37 ergibt sich, indem man 10, 14 und 23 addiert und hiervon 37 subtrahiert. Der Rest ist also 10, wie ganz leicht festzustellen war.

Wie viele - oder besser wie wenige - Leute aber werden wohl dieses Kriterium für Restgleichheit auf die Zahl 782639485 im Kopf anwenden können?

Wenn wir also von der Zweckmäßigkeit der Benutzung von Kriterien für Restgleichheit und Teilbarkeit sprechen, müssen wir von den Schwierigkeiten einzelner Untersuchungen von Zahlen in Bezug auf ihre Teilbarkeit absehen und die Möglichkeiten jedes Kriteriums "im Durchschnitt" bewerten.
Bei einem solchen Herangehen dürfen wir hoffen, ein Maß der Schwierigkeit jedes Kriteriums für Teilbarkeit oder Restgleichheit genau formulieren zu können und sogar das in diesem Sinne beste Kriterium zu finden. Leider haben wir hier keine Möglichkeit, diese Seite des Problems ausführlicher zu behandeln.

13. Alle bisher konstruierten Kriterien für Restgleichheit und Teilbarkeit wirken etwas gekünstelt. Auf den ersten Blick mag es scheinen, als ob diese Kriterien oder wenigstens einige von ihnen zufällig oder durch Probieren gefunden worden seien. In Wirklichkeit ist dem aber nicht so. Es zeigt sich, dass Methoden zur Konstruktion von Teilbarkeits- und Restgleichheitskriterien für jede vorgegebene Zahl existieren.
Sie werden allgemeine Teilbarkeitskriterien bzw. allgemeine Restgleichheitskriterien genannt.

Die allgemeinen Teilbarkeitskriterien sind Methoden, mit deren Hilfe man konkrete Teilbarkeitskriterien erhält. Daher kann man die konkreten Teilbarkeitskriterien als Ergebnisse auffassen, zu denen die allgemeinen Teilbarkeitskriterien führen.
Von diesem Standpunkt aus betrachtet verhalten sich die allgemeinen Teilbarkeitskriterien zu den konkreten ganz so wie ein konkretes Teilbarkeitskriterium zum Ergebnis seiner Anwendung auf eine bestimmte Zahl, d. h. zum Rest einer gegebenen Zahl a bei Division durch eine gegebene Zahl m.

Die allgemeinen Teilbarkeits- und Restgleichheitskriterien erinnern an Algorithmen, und zwar ziemlich eigenartige Algorithmen: Ihre Ergebnisse sind ebenfalls Algorithmen, nämlich die konkreten Teilbarkeits- bzw. Restgleichheitskriterien.
Um jedoch bei den allgemeinen Teilbarkeits- und Restgleichheitskriterien von Algorithmen sprechen zu können, müssen wir uns davon überzeugen, dass sie die notwendigen Bedingungen erfüllen: Sie müssen wohlbestimmt und allgemeingültig sein und zum Ziel führen.

Ausführlicher gesagt, wenn wir ein allgemeines Teilbarkeitskriterium (ebenso wie ein allgemeines Restgleichheitskriterium) erwähnen, müssen wir prüfen, ob folgende Bedingungen erfüllt sind:
Erstens muss es zu jeder Zahl m wirklich ein Kriterium für die Teilbarkeit (Restgleichheit) hinsichtlich dieser Zahl geben.
Es muss also sozusagen jede natürliche Zahl m in das entsprechende Kriterium "verar-

beiten". Gerade darin besteht die Tatsache, dass es zum Ziel führt.

Zweitens muss das allgemeine Kriterium wohlbestimmt sein. Es muss also in Bezug auf eine gegebene Zahl m mit Hilfe eines ganz bestimmten Verfahrens zu einem völlig bestimmten konkreten Kriterium der Teilbarkeit (Restgleichheit) durch diese Zahl m führen.

Drittens schließlich muss ein Kriterium allgemeingültig, d. h. wirklich allgemein sein und ein Teilbarkeits- bzw. Restgleichheitskriterium für jede vorgegebene natürliche Zahl liefern.

In diesem Sinne sind weder die in Abschnitt 2 beschriebene Methode, zu einem Kriterium für Restgleichheit zu kommen, noch die in Abschnitt 6 beschriebene Methode, zu einem Teilbarkeitskriterium zu gelangen, allgemeine Kriterien. Denn die Angabe von Funktionen, die den notwendigen Bedingungen genügen, ist ein Verfahren, das zunächst noch keiner der bekannten Forderungen genügt: wohlbestimmt und allgemeingültig zu sein und zum Ziel zu führen.

Diese Verfahren bieten nämlich keinerlei Garantie dafür, dass die geforderte Funktion gefunden wird, d. h., sie erfüllen nicht die Bedingung, dass sie zum Ziel führen.
Weiterhin kann man die geforderte Funktion, wenn sie existiert, auf verschiedenen Wegen erhalten, ganz abgesehen davon, dass mehrere solcher Funktionen existieren können. Das heißt, diese Verfahren sind nicht wohlbestimmt.
Schließlich sind sie auch nicht allgemeingültig, weil es uns möglicherweise nicht gelingt, die geforderten Funktionen für gewisse Zahlen zu finden.

Das Verfahren selbst sagt in keinem Fall etwas darüber aus. Somit muss das beschriebene Verfahren, damit es zu einem Algorithmus wird, noch durch genaue Hinweise ergänzt werden, welche die Konstruierbarkeit einer völlig bestimmten Funktion f_m für jede konkrete Zahl m garantieren.

Diese "Algorithmisierung" der Konstruktion von Teilbarkeitskriterien kann (sogar ohne große Mühe) durchgeführt werden, und allgemeine Teilbarkeitskriterien sind seit langem bekannt.

Eines dieser allgemeinen Restgleichheitskriterien haben wir praktisch schon in Abschnitt 11 von § 1 aufgestellt, als wir das Problem der Division mit Rest lösten. Wir können es so formulieren:

Jeder positiven ganzen Zahl m lässt sich das Verfahren zuordnen, sukzessive die Zahl m so lange zu subtrahieren, bis sich eine Zahl ergibt, die kleiner als m ist (vgl. den letzten Satz in Abschnitt 1).
Es ist klar, dass dieses Verfahren die notwendigen Eigenschaften besitzt: Es ist wohlbestimmt (wir wissen genau, was der Zahl m zugeordnet ist, nämlich das Verfahren der sukzessiven Subtraktion von m), es ist allgemeingültig (das Verfahren der sukzessiven Subtraktion kann man jedem m zuordnen), und es führt zum Ziel (ein Versuch führt unbedingt zum Erfolg).
Der praktische Wert des beschriebenen allgemeinen Kriteriums der Restgleichheit ist

jedoch nicht sehr groß.

Eine gewisse Vervollkommnung des allgemeinen Kriteriums für Restgleichheit, das auf der sukzessiven Subtraktion beruht, führt auf das bekannte Verfahren der schriftlichen Division von ganzen Zahlen. Dieses Divisionsverfahren kann ebenfalls als allgemeines Kriterium für Restgleichheit angesehen werden.

Es ist nicht überflüssig, daran zu erinnern, dass die überwältigende Mehrheit aller Menschen gerade dieses Kriterium zum Bestimmen des Divisionsrestes benutzt. Dabei werden die Überlegungen nach folgendem Schema durchgeführt, das wir in zwei Varianten wiedergeben, erstens in der Umgangssprache und zweitens in algorithmischer Sprache.

in Umgangssprache	in Algorithmensprache
1. Ich muss den Rest einer gegebenen Zahl a bei Division durch ein gegebenes m bestimmen.	Das allgemeine Restgleichheitskriterium beginnt mit der Verarbeitung der Zahl m.
2. Dazu dividiere ich durch m.	Das allgemeine Kriterium "liefert" das Ergebnis der Verarbeitung der Zahl m: Das konkrete Restgleichheitskriterium hinsichtlich der Division durch m besteht in der unmittelbaren Division durch m.
3. Jetzt beginne ich, a durch m zu dividieren.	Das erhaltene konkrete Kriterium beginnt mit der Verarbeitung der Zahl a.
4. Ich dividiere und erhalte den Rest.	Das konkrete Kriterium führt zum Ziel: zum Rest von a bei Division durch m.

Da bei dieser Betrachtung die ersten drei Schritte sehr einfach sind, darf man sich nicht wundern, dass der vierte Schritt, der faktisch in der Ausführung der Division besteht, bedeutend umfangreicher ist.
Das Ziel, allgemeine Restgleichheits- und Teilbarkeitskriterien zu schaffen, besteht gerade darin, den vierten Schritt auf Kosten des zweiten zu entlasten, indem jener vervollkommnet wird. Gerade das hat man im Auge, wenn man von allgemeinen Teilbarkeits- und Restgleichheitskriterien spricht.

14. Historisch gesehen wurde das erste allgemeine Teilbarkeitskriterium (genauer gesagt sogar ein Restgleichheitskriterium) bereits in der Mitte des 17. Jahrhunderts von dem französischen Mathematiker Blaise Pascal aufgestellt. Das Wesen dieses Kriterium besteht in folgendem:

Es sei m eine natürliche Zahl. Nun bilden wir die Zahlenfolge

$$r_1, r_2, r_3, ... \tag{12}$$

indem wir

r_1 gleich dem Rest von 10 bei Division durch m,
r_2 gleich dem Rest von $10r_1$ bei Division durch m,
r_1 gleich dem Rest von $10r_2$ bei Division durch m,

usw. setzen. Jetzt stellen wir eine beliebige natürliche Zahl A in der Form

$$10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$$

dar und definieren die Funktion

$$F_m(a) = \begin{cases} a_0 + r_1 a_1 + r_2 a_2 + ... + r_n a_n & \text{für } 10^n \geq m \\ \text{Rest bei Division von } A \text{ durch } m & \text{für } 10^n < m \leq A \\ \text{nicht definiert} & \text{für } A < m \end{cases}$$

Aufgabe 47. Man prüfe nach, dass die Funktion F_m für jedes m den Bedingungen a) bis d) aus Abschnitt 2 genügt.

Damit haben wir ein Restgleichheitskriterium für die Division durch ein beliebiges m aufgestellt, d. h. ein allgemeines Restgleichheitskriterium.

Aufgabe 48. Man formuliere die sich aus dem allgemeinen Restgleichheitskriterium von Pascal ergebenden Restgleichheitskriterien bezüglich der Division durch
a) 2, 5 und 10; b) 4, 20 und 25; c) 3 und 9; d) 11; e) 7.

Aufgabe 49. Es sei in der Folge (12)

r_1 gleich dem Rest von 100 bei Division durch m,
r_2 gleich dem Rest von $100r_1$ bei Division durch m,
r_1 gleich dem Rest von $100r_2$ bei Division durch m,

usw. Man entwickle daraus ein allgemeines Restgleichheitskriterium, das dem Restgleichheitskriterium Pascals analog ist.

15. In Abschnitt 12 sprachen wir über den Vergleich der Güte von Teilbarkeitskriterien (bzw. Restgleichheitskriterien) für eine gegebene Zahl. Da ein allgemeines Teilbarkeitskriterium uns Teilbarkeitskriterien für jede natürliche Zahl liefern muss, ist es nicht verwunderlich, dass es für verschiedene Zahlen auf Teilbarkeitskriterien höchst unterschiedlicher Güte führen kann.

So liefert zum Beispiel das Pascalsche allgemeine Kriterium nicht nur recht annehmbare Restgleichheitskriterien hinsichtlich der Division durch 3 und 11, sondern in Bezug auf die Anwendung für die Division durch 7 auch ein recht umständliches und unzweckmäßiges (vgl. Aufgabe 48e).

In diesem Zusammenhang kann man für die allgemeinen Teilbarkeitskriterien (bzw; Restgleichheitskriterien) Überlegungen anstellen, die denen ähnlich sind, die wir im Abschnitt 12 bei der Behandlung der Güte konkreter Teilbarkeitskriterien durchgeführt haben.
In diesem Sinne muss als bestes allgemeines Kriterium der Teilbarkeit bzw. Restgleichheit ein solches Kriterium angesehen werden, welches bei der Anwendung auf eine beliebig vorgegebene positive ganze Zahl m das beste Kriterium der Teilbarkeit bzw. Restgleichheit für dieses m liefert.

Der Leser muss sich aber darüber im klaren sein, dass das Problem, das beste allgemei-

ne Teilbarkeitskriterium aufzustellen, nicht nur von seiner Lösung, sondern sogar von seiner strengen Formulierung weit entfernt ist.

4 Die Teilbarkeit von Potenzen

I. Die Frage nach der Teilbarkeit von Potenzen ist im Grunde genommen eine Frage nach der Teilbarkeit eines Produktes, und zwar eines Produktes mehrerer gleicher Faktoren. Daher kann man diese Frage auf, der Grundlage der Ergebnisse von § 2 beantworten. Im Fall großer Exponenten führt eine Verkleinerung der Basis der Potenz jedoch noch nicht gleich zum Auffinden des Bestes bei der Division der Potenz, und wir müssen mehrere Kunstgriffe anwenden (vgl. die Beispiele in 52, Abschnitt 2).

Außerdem haben wir bei der Bildung allgemeiner Teilbarkeitskriterien sukzessive die Reste von Potenzen von 10^k bei Division durch m berechnet. Obwohl dieser Prozess an und für sich nicht kompliziert ist, zeigt er jedoch noch keinerlei Gesetzmäßigkeiten in der Folge (12) und liefert auch keine Möglichkeit dafür, die Zahl k so festzulegen, dass alle Reste klein genug sind (übrigens existiert eine solche Möglichkeit; ferner zeigt sich, dass die Zahl k so gewählt werden kann, dass alle diese Reste gleich 1 sind).

Alles bisher Gesagte zeigt, dass es notwendig ist, sich mit dem Studium der Teilbarkeit von Potenzen ausführlicher zu beschäftigen.

2. Wir wollen nun unsere Kenntnisse auf dem Gebiet der Zahlentheorie noch ein wenig erweitern.

Satz 19 (Satz von Fermat). Ist p eine Primzahl, dann ist die Differenz $a^p - a$ durch p teilbar.

Diesen "kleinen Fermatschen Satz" darf man nicht mit dem "großen Fermatschen Satz" verwechseln. Der letztere sagt aus, dass für ganzes $n > 2$ keine ganzen Zahlen a, b und c existieren, für welche $a^n + b^n = c^n$ gilt. Trotz zahlreicher Versuche konnte der große Fermatsche Satz bis jetzt weder bewiesen noch widerlegt werden. Daher spricht man vielfach von der Fermatschen Vermutung.

Folgerung. Ist p eine Primzahl und a nicht durch p teilbar, so ist $a^{p-1} - 1$ durch p teilbar.

Aufgabe 50. Man zeige an einem konkreten Beispiel, dass sowohl der Satz 19 als auch die Folgerung daraus für zusammengesetztes p falsch ist.

Aufgabe 51. Man beweise den Fermatschen Satz unter Zuhilfenahme des Ergebnisses der Aufgabe 26.

Gegeben sei ein natürliches m in der kanonischen Zerlegung

$$m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} \tag{13}$$

wir setzen

$$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) ... p_k^{\alpha_k - 1}(p_k - 1) \tag{14}$$

Die Formeln (13) und (14) ordnen jeder natürlichen Zahl m eine wohldefinierte Zahl $\varphi(m)$ zu. Das bedeutet, dass wir von einer Funktion φ mit natürlichem Argument sprechen können. Solche Funktionen werden als als zahlentheoretische Funktionen bezeichnet.

Definition. Die soeben definierte Funktion φ wird Eulersche Funktion genannt.

Die Eulersche Funktion spielt in vielen Fragen der Zahlentheorie eine höchst wichtige Rolle. Auch in unserem Büchlein werden wir auf einige Anwendungen dieser Funktion eingehen.

Satz 20. Sind m_1 und m_2 teilerfremd, dann gilt die Gleichung

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$$

Aufgabe 52. Man berechne $\varphi(12)$, $\varphi(20)$, $\varphi(100)$.

Aufgabe 53. Man bestimme alle Zahlen m, für welche
a) $\varphi(m) = 10$, b) $\varphi(m) = 8$ gilt.

Aufgabe 54. Man beweise, dass kein m mit $\varphi(m) = 14$ existiert.

Aufgabe 55. Man beweise, dass $\varphi(m)$ gleich der Anzahl der zu m teilerfremden natürlichen Zahlen ist, welche kleiner als m sind. (Diese Eigenschaft der Eulerschen Funktion ist außerordentlich wichtig. Sie wird häufig als Definition dieser Funktion verwendet.)

Satz 21 (Satz von Euler). Sind die Zahlen a und m teilerfremd, dann ist $a^{\varphi(m)} - 1$ durch m teilbar.

3. Durch Anwendung dieser Sätze gelangen wir zu einigen allgemeinen Kriterien für Teilbarkeit und Restgleichheit.

Es sei m eine feste natürliche Zahl und A dargestellt in der Form

$$A = a_0 + a_1 10^{\varphi(m)} + a_2 10^{2\varphi(m)} + ... + +a_k 10^{k\varphi(m)}$$

wobei $0 \leq a_0, a_1, a_2, ...a_k \leq 10^{\varphi(m)}$ ist, d. h., die Zahlen a_i $(i = 0, 1, ..., k)$ seien $\varphi(m)$-stellig. Die durch

$$F(A) = \begin{cases} a_0 + a_1 + a_2 + ... + a_k & \text{für } A \geq 10^{\varphi(m)} \\ \text{Rest bei Division von } A \text{ durch } m & \text{für } m \leq A < 10^{\varphi(m)} \\ \text{nicht definiert} & \text{für } A < m \end{cases}$$

definierte Funktion F liefert, wie leicht zu erkennen ist, ein allgemeines Restgleichheitskriterium.

Aufgabe 56. Man beweise diese Behauptung.

Satz 22. Sind die Zahlen a und m teilerfremd und die Zahlen k_1 und k_2 restgleich hinsichtlich der Division durch $\varphi(m)$, dann sind die Zahlen a^{k_1} und a^{k_2} restgleich hinsichtlich der Division durch m.

Aufgabe 57. Man beweise, dass $n^{13} - n$ durch 2730 teilbar ist.

4. Das soeben angegebene allgemeine Restgleichheitskriterium ist nicht in allen Fällen hinreichend "ökonomisch", weil die Zahl $\varphi(m)$ im allgemeinen recht groß sein kann. Daher muss man bei der Benutzung des Kriterium einerseits große Zahlen addieren und andererseits $\varphi(m)$-stellige Zahlen direkt durch m dividieren (oder aber irgendein anderes Teilbarkeits- bzw. Restgleichheitskriterium anwenden).

Es empfiehlt sich deshalb, statt $\varphi(m)$ einen anderen, und zwar kleineren Exponenten zu verwenden. In manchen Fällen gelingt das auch. So kann man zum Beispiel bei $m = 37$ anstelle von $\varphi(m) = 36$ den Exponenten 3 nehmen, weil 1000 bei Division durch 37 den Rest 1 liefert.
Bei m $= 11$ könnte anstelle von $\varphi(m) = 10$ der Exponent 2 genommen werden usw.

Definition. Die kleinste Zahl δ, für welche a^δ bei Division durch m den Rest 1 liefert, heißt der Exponent, zu dem die Zahl a hinsichtlich der Division durch m mit Rest gehört.
Oft sagt man, diese Zahl sei der Exponent, zu dem die Zahl a mod m gehört.

Für beliebige teilerfremde Zahlen a und m ist der Exponent, zu dem die Zahl a hinsichtlich der Division durch m gehört, höchstens gleich $\varphi(m)$. Eben diesen Exponenten kann man anstelle von $\varphi(m)$ in der Formulierung des allgemeines Teilbarkeitskriteriums aus Abschnitt 3 nehmen.

Aufgabe 58. Man modifiziere die Konstruktion des allgemeinen Teilbarkeitskriteriums, indem man statt $\varphi(m)$ den Exponenten benutzt, zu dem die Zahl 10 hinsichtlich der Division durch m mit Rest gehört.

5. Die Bedeutung der Eulerschen Funktion und des Eulerschen Satzes erschöpft sich nicht in Teilbarkeitskriterien. Mit ihrer Hilfe kann man z. B. sogenannte diophantische Gleichungen lösen.

Satz 23. Sind die Zahlen a und b teilerfremd, so ist die Gleichung

$$ax + by = c \tag{15}$$

in ganzen Zahlen immer lösbar, und ihre ganzzahligen Lösungen sind die Zahlenpaare (x_t, y_t) mit

$$x_t = ca^{\varphi(b)-1} + bt \qquad , \qquad y_t = c\frac{1 - a^{\varphi(b)}}{b} - at$$

wobei t eine beliebige ganze Zahl ist.

Aufgabe 59. Man beweise einen zu Satz 23 analogen Satz, ohne vorauszusetzen, dass die Zahlen a und b teilerfremd sind.

Aufgabe 60. Auf der Grundlage des Ergebnisses von Aufgabe 29 ermittle man eine Lösungsmethode für diophantische Gleichungen der Form (15).

Aufgabe 61. Man löse folgende Gleichungen in ganzen Zahlen:
a) $5x + 7y = 9$, b) $25x + 13y = 8$.

6. Satz 24. Es sei m zu 10 teilerfremd, und k sei mit $10^{\varphi(m)-1}$ restgleich hinsichtlich der Division durch m. Dann sind die Zahlen $10a + b$ und $a + kb$ teilbarkeitsgleich in Bezug auf m.

Stützt man sich auf diesen Satz, dann kann man folgendes allgemeine Teilbarkeitskriterium bilden: Wir bezeichnen den Rest von $10^{\varphi(m)-1}$ bei Division durch m mit k', stellen die beliebige Zahl A in der Form $10a + b$ $(0 \leq b < 10)$ dar und setzen

$$F(A) = \begin{cases} a + k'b & \text{für } A > a + k'b \\ \text{Rest bei Division von } A \text{ durch } m & \text{für } m \leq A < a + k'b \\ \text{nicht definiert} & \text{für } A < m \end{cases}$$

Ist k' sehr groß (d.h. ist die Differenz von m und k' klein), so ist es zweckmäßig, in der Formulierung des entsprechenden Kriteriums $k' - m$ statt k' zu nehmen.

Aufgabe 62. Man prüfe nach, ob für die Funktion F die Bedingungen a) bis c) und d*) erfüllt sind.

Aufgabe 63. Aufgrund des soeben gebildeten allgemeinen Teilbarkeitskriteriums leite man Kriterien für Teilbarkeit durch 17, 19, 27, 29, 31, 49 her.

Aufgabe 64. Man bilde ein ähnliches allgemeines Teilbarkeitskriterium, indem man eine beliebige natürliche Zahl in der Form $100a + b$ $(0 \leq b < 100)$ darstellt, und leite daraus Kriterien für Teilbarkeit durch 17, 43, 49, 67, 101, 199 her.

5 Beweise der Sätze

1. Es genügt, darauf hinzuweisen, dass $a = a \cdot 1$ gilt.

2. Nach Voraussetzung lassen sich Zahlen d_1 und d_2 finden, für welche $a = bd_1$ und $b = cd_2$ gilt. Dann ist aber

$$a = cd_1d_2, \qquad \text{d.h.} \quad c|a$$

3. Nach Voraussetzung ist $a = bc_1$ und $b = ac_2$; hieraus folgt $a = ac_1c_2$, also $c_1c_2 = 1$. Da nach Voraussetzung die Zahlen c_1 und c_2 ganz sind, gilt entweder $c_1 = c_2 = 1$ oder $c_1 = c_2 = -1$.
Im ersten Fall ist $a = b$, im zweiten ist $a = -b$.

4. Es sei $a = bc$. Wäre $|c| \geq 1$, so müsste wegen $|b| > |a|$ auch $|bc| \geq |a|$ sein. Das steht jedoch im Widerspruch zur Annahme. Also muss $|c|$ kleiner als 1 sein. Da c nach Voraussetzung aber eine ganze Zahl ist, muss $c = 0$ sein, und somit ist auch $a = 0$.

5. Aus $a = bc$ folgt offensichtlich $|a| = |b||c|$ und umgekehrt, wobei die Zahlen c und $|c|$ zugleich ganz oder nicht ganz sind.

6. Nach Voraussetzung gilt

$$a_1 = bc_1, \quad a_2 = bc_2, \quad ..., \quad a_n = bc_n$$

wobei alle Zahlen $c_1, c_2, ..., c_n$ ganz sind. Addiert man diese Gleichungen, so erhält man

$$a_1 + a_2 + ... + a_n = b(c_1 + c_2 + ... + c_n)$$

In der Klammer steht eine ganze Zahl, was zu beweisen war.

8. Wir führen den Beweis indirekt. Angenommen, es gäbe nur endlich viele Primzahlen; man könnte sie also aufschreiben:

$$p_1, p_2, ..., p_n \tag{16}$$

Das Produkt dieser Zahlen wollen wir mit P bezeichnen. Nun betrachten wir die Differenz $P - 1$. Diese Differenz ist größer als jede der in (16) enthaltenen Primzahlen und kann daher selbst keine Primzahl sein. Demzufolge ist sie durch mindestens eine Primzahl p_k teilbar.
Da aber aufgrund der Folgerung aus Satz 6 die Zahl P ebenfalls durch p_k teilbar ist, muss auch $p_k|1$ gelten. Daraus folgt aber $p_k = 1$, was der Annahme widerspricht, dass p_k eine Primzahl ist.
Der Gedankengang dieses Beweises für die Unendlichkeit der Menge der Primzahlen stammt von Euklid (4. Jh. v.u.Z.).

9. Sind die Zahlen a und p teilerfremd, so ist der Satz bewiesen. - Sind diese beiden Zahlen aber nicht teilerfremd, so müssen sie beide durch eine Zahl teilbar sein, welche von 1 verschieden ist. Da p Primzahl ist, kann diese Zahl nur p selbst sein. Das heißt für unseren Fall $p|a$, was zu beweisen war.

10. Teilen wir M mit Rest durch m, dann erhalten wir

$$M = mq + r$$

wobei $0 \leq r < m$ ist. Da sowohl M als auch m durch a und durch b teilbar sind, muss nach der Folgerung aus Satz 6 auch die Zahl r durch diese beiden Zahlen teilbar sein; r ist also ein gemeinsames Vielfaches von a und b.
Wegen $r < m$ ist m das kleinste positive gemeinsame Vielfache der Zahlen a und b. Daher kann r nicht positiv sein; also ist $r = 0$. Somit ist M durch m teilbar.

11. Die Zahlen a und b seien teilerfremd und m ihr kleinstes gemeinsames Vielfaches. Wegen $a|ab$ und $b|ab$ gilt nach dem vorhergehenden Satz auch $m|ab$.
Es sei $ab = mk$. Setzen wir $m = ac$ an, dann ist $ab = ack$, also $b = ck$, so dass $k|b$ gilt. Ebenso können wir uns davon überzeugen, dass $k|a$ ist.
Da nach Voraussetzung die Zahlen a und b teilerfremd sind, muss $k = 1$ sein, und das bedeutet, dass $m = ab$ ist.

12. Das kleinste gemeinsame Vielfache der Zahlen b und c bezeichnen wir mit m. Nach dem vorhergehenden Satz ist $m = bc$.
Nach Voraussetzung ist $c|ab$ und darüber hinaus offenbar $b|ab$. Nach Satz 10 heißt das $bc|ab$, also $ab = bck$ oder (nach Kürzen durch b) $a = ck$, was zu zeigen war.

13. Der Beweis wird durch Induktion nach der Anzahl der Faktoren geführt. Ist die Anzahl der Faktoren gleich 1, dann ist der Satz trivial.
Wir nehmen an, der Satz sei für jedes Produkt von n Faktoren bewiesen, und $a_1a_2...a_na_{n+1}$ sei durch p teilbar. Bezeichnen wir das Produkt $a_1a_2...a_n$ mit A, dann gilt also $p|Aa_{n+1}$. Ist $p|a_{n+1}$, so ist der Satz bewiesen. Andernfalls sind nach Satz 9 die Zahlen a_{n+1} und p teilerfremd. Dann gilt aber nach dem Vorangehenden $p|A$. Da A ein Produkt aus n Faktoren ist, muss nach Induktionsvoraussetzung einer dieser Faktoren durch p teilbar sein, womit der Satz bewiesen ist.

Folgerung. Der Bruch selbst ist eine ganze Zahl, d. h., sein Zähler ist durch den Nenner teilbar.
Nehmen wir an, der Zähler sei das Produkt aus den beiden Faktoren p und $1 \cdot 2 \cdot 3 \cdot ... (p-1) = (p-1)!$. Keiner der Faktoren im Nenner des Bruches ist durch p teilbar. Nach dem vorhergehenden Satz ist somit auch der gesamte Nenner nicht durch p teilbar.
Dann aber ist er nach Satz 9 zu p teilerfremd. Folglich muss der zweite Faktor des Zählers durch den Nenner teilbar sein. Bezeichnen wir den Quotienten bei dieser Division mit q, dann erhalten wir $\binom{p}{k} = pq$, und die Behauptung ist bewiesen.

14. Zunächst zeigen wir, dass es möglich ist, jede von 1 verschiedene Zahl in Primfaktoren zu zerlegen.
Wir nehmen an, alle Zahlen, die kleiner als N sind, könnten so zerlegt werden. Ist die Zahl N eine Primzahl, dann ist sie automatisch in Primzahlen zerlegbar (nämlich in ein Produkt, das nur den einzigen Faktor N enthält), und der Satz ist bewiesen.

Nun sei N eine zusammengesetzte Zahl, N_1 ein Teiler von N, der sowohl von N als auch von 1 verschieden ist, und N_2 der Quotient bei Division von N durch N_1.

Dann ist $N = N_1 N_2$, wobei, wie man leicht sieht, $1 < N_2 < N$ gilt. Da N_1 und N_2 kleiner sind als N, sind sie nach Voraussetzung Produkte von Primzahlen. Sind $N_1 = p_1 p_2 ... p_k$ und $N2 = q_1 q_2 ... q_l$ diese Zerlegungen, dann ist $p_1 p_2 ... p_k q_1 q_2 ... q_l$ die gesuchte Zerlegung der Zahl N, und die Möglichkeit der Zerlegung ist damit bewiesen.

Nun führen wir den Beweis für die Eindeutigkeit dieser Zerlegung. Es seien die beiden Zerlegungen $p_1 p_2 ... p_k$ und $q_1 q_2 ... q_l$ der Zahl N in Primfaktoren gegeben. Offenbar ist

$$p_1 p_2 ... p_k = q_1 q_2 ... q_l \tag{17}$$

Da das Produkt $q_1 q_2 ... q_l$ durch p_1 teilbar ist, ist nach dem vorangehenden Satz mindestens einer der Faktoren $q_1, q_2, ..., q_l$ durch p_1 teilbar. Es sei etwa $p_1 | q_1$. (Dass wir gerade den ersten Faktor auf der rechten Seite (17) als durch p_1 teilbar annehmen, bedeutet durchaus keine zusätzliche Voraussetzung, da wir ja auf der rechten Seite die Faktoren miteinander vertauschen, also umnummerieren können, so dass der durch p_1 teilbare Faktor an die erste Stelle kommt, also mit q_1 bezeichnet werden darf.)

Da aber alle Faktoren - und damit auch q_1 - Primzahlen sind, ist das nur für $p_1 = q_1$ möglich. Kürzen wir die Gleichung (17) durch p_1, so erhalten wir

$$p_2 p_3 ... p_k = q_2 q_3 ... q_l \tag{18}$$

Ähnlich dem Vorhergehenden überzeugen wir uns davon, dass eine der Zahlen $q_2, q_3, ..., q_l$, (zum Beispiel q_2) durch p_2 teilbar ist, also $q_2 = p_2$ gelten muss. Kürzen wir (18) durch p_2, so verringert sich die Anzahl der Faktoren auf beiden Seiten wieder um 1.
Diesen Kürzungsprozess kann man so lange fortführen, bis sich eines dieser Produkte völlig weggekürzt hat. Angenommen, das in (17) links stehende Produkt sei als erstes weggekürzt.

Dann muss sich auch das rechts stehende Produkt völlig mit weggekürzt haben, weil wir sonst eine Gleichung der Form

$$1 = q_{k+1} q_{k+2} ... q_l$$

erhalten würden; das ist unmöglich, da die Eins nicht durch eine Primzahl teilbar ist. Somit haben wir die Beziehungen

$$p_1 = q_1, p_2 = q_2, ..., p_k = q_k$$

erhalten, womit der Satz vollständig bewiesen ist

15. Es sei $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ die kanonische Zerlegung von a bzw. $q_1^{\beta_1} q_2^{\beta_2} ... q_l^{\beta_l}$ die von b; ferner sei d ein gemeinsamer Teiler dieser Zahlen. Ist $d \neq 1$, so muss d durch eine Primzahl p teilbar sein. Nach Satz 3 gilt dann $p|a$ und $p|b$, so dass p sowohl eine der Zahlen $p_1, p_2, ..., p_k$ als auch eine der Zahlen $q_1, q_2, ..., a_l$ ist. Daher muss unter den Primzahlen der kanonischen Zerlegung von a wenigstens eine vorkommen, die auch in der kanonischen Zerlegung von b auftritt. Sind dagegen a und b teilerfremd und kommt p in der kanonischen Zerlegung von a vor, so ist b nicht durch p teilbar, so dass p nicht in der kanonischen Zerlegung von b auftreten kann.

16. Die Bedingung ist notwendig; denn wegen $p_i^{\alpha_i}|a$ $(i = 1, 2, ..., k)$ ergibt sich aus $a|b$ die Behauptung einfach durch Hinweis auf Satz 2. Dass die Bedingung hinreichend ist, wird durch vollständige Induktion bewiesen.
Die Teilbarkeitsrelation $p_1^{\alpha_1}|b$ ist eine der Voraussetzungen. Wir nehmen nun an, wir hätten schon bewiesen, dass

$$p_1^{\alpha_1}...p_l^{\alpha_l}|b \qquad (1 \leq l \leq k)$$

ist. Nach unseren Annahmen gilt aber auch $p_{l+1}^{\alpha_{l+1}}|b$. Da nach vorigem Satz die Zahlen $p_1^{\alpha_1}...p_l^{\alpha_l}$ und $p_{l+1}^{\alpha_{l+1}}$ teilerfremd sind, können wir die Folgerung aus Satz 11 anwenden; diese liefert uns die Beziehung

$$p_1^{\alpha_1}...p_l^{\alpha_l}p_{l+1}^{\alpha_{l+1}}|b$$

Damit ist der Induktionsschritt begründet.

17. Die Bedingung ist notwendig: Es sei

$$a = mq_1 + r_1 \qquad (0 \leq r_1 < m) \tag{19}$$
$$b = mq_2 + r_2 \qquad (0 \leq r_2 < m) \tag{20}$$

Da a und b restgleich sind, muss $r_1 = r_2$ sein. Das bedeutet aber

$$a - b = m(q_1 - q_2)$$

also $m|(a - b)$, die Differenz ist durch m teilbar.
Die Bedingung ist auch hinreichend: Es sei also $m|(a-b)$. Dividieren wir a und b durch m mit Rest, so erhalten wir (19) bzw. (20). Hierbei ist

$$a - b = m(q_1 - q_2) + r_1 - r_2 \qquad \text{also} \qquad (a - b) - m(q_1 - q_2) = r_1 - r_2$$

Nach Satz 6 gilt $m|(r_1 - r_2)$. Nun ist aber $|r_1 - r_2| < m$. Nach Satz 4 folgt daraus $r_1 - r_2 = 0$, also $r_1 = r_2$, was zu beweisen war.

18. Aus der Voraussetzung erhalten wir nach Satz 16

$$\begin{aligned} a_1 &= b_1 + mq_1 \\ a_2 &= b_2 + mq_2 \\ &... \\ a_n &= b_n + mq_n \end{aligned} \tag{21}$$

Wenn wir diese Gleichungen seitenweise addieren, ergibt sich nach einfachen Umformungen

$$(a_1 + a_2 + ... + a_n) - (b_1 + b_2 + ... + b_n) = m(q_1 + q_2 + ... + q_n)$$

Nach Satz 17 besagt das aber, dass die Summen restgleich sind. Zum Beweis, dass die Produkte restgleich sind, verwenden wir die Identität

$$(k + lm)(p + qm) = kp + (kq + lp + lqm)m$$

Daraus folgt, dass das Produkt zweier Zahlen der Gestalt $a + bm$ wieder eine Zahl der gleichen Form ist. Durch einen Induktionsschluss überzeugen wir uns davon, dass auch das Produkt beliebig vieler Zahlen der Gestalt $a + bm$ ebenfalls eine Zahl dieser Form ist. Multiplizieren wir jetzt alle Gleichungen von (21) seitenweise und wenden die soeben durchgeführten Überlegungen auf die rechte Seite an, so erhalten wir

$$a_1 a_2 ... a_n = b_1 b_2 ... n_n + mt$$

wobei t eine ganze Zahl ist. Damit ist bewiesen, dass die Produkte restgleich sind.

19. Der Beweis wird durch vollständige Induktion nach a geführt. Für $a = 1$ gilt

$$a^p - a = 1 - 1 = 0$$

und 0 ist ja durch p teilbar. Wir nehmen an, $a^p - a$ sei durch p teilbar, und beweisen, dass auch $(a+1)^p - (a+1)$ durch p teilbar ist. Wenn wir $(a+1)^p$ nach dem binomischen Satz ausrechnen, erhalten wir

$$\begin{aligned}(a+1)^p - (a+1) &= a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + ... + \binom{p}{p-1} a + 1 - a - 1 \\ &= a^p - a + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + ... + \binom{p}{p-1} a \qquad (22)\end{aligned}$$

Nach Voraussetzung ist $a^p - a$ durch p teilbar. Nach der Folgerung aus Satz 13 kann geschlossen werden, dass $\binom{p}{k}$, $1 \leq k \leq p-1$, ebenfalls durch p teilbar ist. Demzufolge ist jeder Summand der Summe (22) durch p teilbar, also (nach Satz 6) auch die gesamte Summe. Der Induktionsschritt ist also begründet und der ganze Satz damit bewiesen.

Folgerung. Nach dem Satz von Fermat gilt

$$p | (a^p - a) = a(a^{p-1} - 1)$$

Ist a nicht durch p teilbar, so muss $a^{p-1} - 1$ durch p teilbar sein (nach Satz 13).

20. Es sei $m_1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ und $m_2 = q_1^{\beta_1} q_2^{\beta_2} ... q_l^{\beta_l}$. Nach Satz 15 ist jede der Zahlen $p_1, ..., p_k$ von jeder der Zahlen $q_1, ..., q_l$ verschieden. Die kanonische Zerlegung von $m_1 m_2$ ist also $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} ... q_l^{\beta_l}$. Daher gilt

$$\varphi(m_1 m_2) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) ... p_k^{\alpha_k - 1}(p_k - 1) q_1^{\beta_1 - 1}(q_1 - 1) q_2^{\beta_2 - 1}(q_2 - 1) ... q_k^{\beta_l - 1}(q_l - 1)$$

also

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$$

21. Wir beweisen zuerst durch Induktion nach α, dass $a^{p^{\alpha-1}(p-1)} - 1$ durch p^α teilbar ist.
Für $\alpha = 1$ ist die zu beweisende Behauptung offenbar eine Folgerung aus dem Fermatschen Satz, den wir schon bewiesen haben. Die Induktionsbasis ist damit gesichert.

Wir nehmen jetzt an, es gelte $p|(a^{p^{\alpha-1}(p-1)}-1)$, und betrachten den Ausdruck $a^{p^\alpha(p-1)}$. Wir müssen beweisen, dass er durch $^{\alpha+1}$ teilbar ist. Nun ist aber

$$a^{p^\alpha(p-1)}-1=(a^{p^{\alpha-1}(p-1)})^p-1$$

Da $a^{p^{\alpha-1}(p-1)}-1$ nach Voraussetzung durch p^α teilbar ist, hat die Zahl $a^{p^{\alpha-1}(p-1)}$ die Form $Np^\alpha+1$. Also ist

$$a^{p^\alpha(p-1)}=(Np^\alpha+1)^p-1$$

oder nach dem binomischen Satz

$$a^{p^\alpha(p-1)}=N^pp^{\alpha p}+\binom{p}{1}N^{p-1}p^{\alpha(p-1)}+...+\binom{p}{p-1}Np^\alpha+1-1$$

Der erste Summand dieser Summe ist durch $p^{\alpha+1}$, da er durch $p^{\alpha p}$ teilbar ist und $\alpha p\geq\alpha+1$ gilt. In jedem der $p-1$ Summanden, welche noch folgen, ist p mit einem Exponenten enthalten, der mindestens gleich α ist, und außerdem ist nach Satz 13 der zugehörige Binomialkoeffizient durch p teilbar.
Also ist jeder dieser Summanden durch $p^{\alpha+1}$ teilbar. Schließlich kann die Differenz $1-1=0$ unberücksichtigt gelassen werden. Daher gilt nach Satz 6

$$p^{\alpha+1}|(a^{p^\alpha(p-1)}-1)$$

Der Fall, dass die Zahl m nur einen einzigen Primteiler hat, ist somit geklärt.

Wir nehmen jetzt an, der Eulersche Satz sei für die Exponenten m_1 und m_2 bewiesen, und diese beiden Zahlen seien teilerfremd.
Wir beweisen nun den Eulerschen Satz für den Exponenten $m=m_1m_2$. Setzen wir $m_1=p_1^{\alpha_1}...p_k^{\alpha_k}$ und $m_2=p_{k+1}^{\alpha_{k+1}}$, so erhalten wir offensichtlich genau den Induktionsschritt, der zur Vervollständigung des Beweises für den Satz notwendig ist. Damit ist die formulierte Teilbehauptung bewiesen.

Sind die Zahlen a und m teilerfremd, dann ist a auch zu m_1 teilerfremd. Das bedeutet aber, dass auch $a^{\varphi(m_2)}$ zu m_1 teilerfremd ist. Nach Voraussetzung ist daher

$$(a^{\varphi(m_2)})^{\varphi(m_1)}-1=a^{\varphi(m_2)\varphi(m_1)}-1=a^{\varphi(m_1m_2)}-1=a^{\varphi(m)}-1$$

durch m_1 teilbar. Ebenso überzeugen wir uns davon, dass $a^{\varphi(m)}-1$ durch m_2 teilbar ist. Da aber die Zahlen m_1 und m_2 zueinander teilerfremd sind, ist $a^{\varphi(m)}-1$ auch durch ihr Produkt, also durch m teilbar. Der Eulersche Satz ist damit bewiesen.

22. Es sei

$$k_1=\varphi(m)q_1+r\qquad,\qquad k_2=\varphi(m)q_2+r$$

Dann ist

$$a^{k_1}=a^{\varphi(m)q_1+r}-(a^{\varphi(m)})^{q_1}a^r$$

Nach dem Eulerschen Satz und Satz 18 ist $a^{\varphi(m)q_1}a^r$ hinsichtlich der Division durch m restgleich. Analog beweist man, dass die Zahlen a^{k_2} und a^r hinsichtlich der Division

durch m restgleich sind. Das bedeutet aber, dass auch die Zahlen a^{k_1} und a^{k_2} hinsichtlich der Division durch m restgleich sind.

23. Wir wollen zunächst wenigstens eine Lösung (x', y') dieser Gleichung ermitteln. Hierzu genügt es offenbar, eine Zahl x' zu bestimmen, für die $b|(ax' - c)$ gilt.
Nach dem Eulerschen Satz ist $a^{\varphi(b)} - 1$ durch b teilbar, also $b|(ca^{\varphi(b)} - c)$; daher kann für x' die Zahl $ca^{\varphi(b)-1}$ genommen werden.

Nun sei (x'', y'') eine andere Lösung der Gleichung $ax + by = c$. Wir werden zeigen, dass die Zahlen x' und x'' hinsichtlich der Division durch b restgleich sind. In der Tat ist

$$ax' + by' = c \qquad , \qquad ax'' + by'' = c$$

Subtrahieren wir die zweite Zeile von der ersten, so erhalten wir

$$a(x' - x'') - b(y' - y'') = 0$$

also $b|a(x' - x'')$. Da a und b nach Voraussetzung teilerfremd sind, gilt nach Satz 12 die Beziehung $b|(x' - x'')$, und wir brauchen uns nur noch auf den Satz 17 zu berufen. Somit befinden sich alle gesuchten Werte für m unter den Zahlen

$$x_t = ca^{\varphi(b)-1} + bt$$

Da jedoch $b|(ax_t - c)$ gilt, können wir, wenn wir noch

$$y_t = \frac{-ax_t + c}{b} = c\frac{1 - a^{\varphi(b)}}{b} - at$$

setzen, feststellen, dass alle Zahlenpaare (x_t, y_t) tatsächlich Lösungen unserer Gleichung sind.

24. Da die Zahlen m und 10 zueinander teilerfremd sind, sind die Zahlen $10a + b$ und $(10a + b)10^{\varphi(m)-1}$ nach Satz 15 teilbarkeitsgleich in Bezug auf m. Nun gilt aber

$$(10a + b)10^{\varphi(m)-1} = 10^{\varphi(m)}a + 10^{\varphi(m)-1}b$$

so dass nach dem Eulerschen Satz und nach Satz 18 die Zahlen $10a + b$ und $a + kb$ in Bezug auf m teilbarkeitsgleich sind.

6 Lösungen der Aufgaben

1. Es gilt $0 = a \cdot 0$ für jedes a, also $a|0$.

2. Es gilt $a = 1 \cdot a$, also $1|a$.

3. Es sei $a|1$. Das bedeutet $1 = ac$, c eine ganze Zahl. Hieraus folgt $|a| \leq 1$. Da aber $a \neq 0$ sein sollte, muss $a = \pm 1$ sein.

4. Es genügt, ein beliebiges $c > 1$ zu nehmen und $b = ac$ zu setzen.

5. Die Zahl $2a$ beispielsweise ist ein solches b.
Beweis. Für irgendein c möge also sowohl $c|2a$ als auch $a|c$ gelten. Das bedeutet, dass es Zahlen d_1 und d_2 gibt, für welche $2a = d_1 c$ und $c = d_2 a$ gilt. Hieraus folgt $2a = d_1 d_2 a$ oder, nach Kürzen von a,

$$2 = d_1 d_2$$

Für ganze d_1 und d_2 ist diese Gleichung jedoch nur zu erfüllen, wenn der eine Faktor 1 und der andere 2 ist. Ist $d_1 = 1$, so ist $c = 2a = b$. Ist jedoch $d_2 = 1$, dann ist $c = a$.

6. Die Beweise unterscheiden sich in keiner Weise von denen für die gewöhnliche Division.

7. Es sei n eine feste Zahl größer als 1. Wir setzen $b|_n a$, wenn ein c existiert, für welches $a = bc$ und $c \leq n$ ist. Die Gültigkeit der Sätze, die den Sätzen 1, 3 und 4 analog sind, lässt sich mühelos nachprüfen.
Setzen wir jetzt jedoch $a = nb$ und $b = nc$, dann gilt $b|_n a$ und $c|_n b$. In diesem Fall ist $a = n^2 c$. Da aber $n^2 > n$ ist, gilt weder $c|_n a$ noch $b|_(a + a)$.

8. a) Es seien zwei Minimalzahlen a_1 und a_2 gegeben. Aufgrund der Dichotomie ist entweder $a_1 \geq a_2$ oder $a_2 \geq a_1$. Für $a_1 \geq a_2$ folgt daraus, dass a_1 minimal ist, $a_1 = a_2$. Ist jedoch $a_2 \geq a_1$, so folgt $a_1 = a_2$ daraus, dass a_2 minimal ist.

b) Es sei a eine Zahl, und b_1 und b_2 seien zwei ihr unmittelbar vorangehende Zahlen. Aufgrund der Dichotomie muss entweder $b_1 \geq b_2$ oder $b2 \geq b_1$ sein.
Wir nehmen einmal $b_1 \geq b_2$ an. Ist $a \geq b_1 \geq b_2$, so muss, da die Zahl b_2 der Zahl a unmittelbar vorangeht, entweder $b_1 = a$ oder $b_1 = b_2$ sein. Nach Voraussetzung ist aber $b_1 \neq a$; also ist $b_1 = b_2$ und damit die geforderte Eindeutigkeit bewiesen.

c) Unter einem unmittelbaren Nachfolger einer Zahl a versteht man eine Zahl b, für welche $b \geq a$ und $b \neq a$ gilt und für welche aus $b \geq c \geq a$ entweder $c = b$ oder $c = a$ folgt.
Nehmen wir einmal an, ein gewisses a habe keinen unmittelbaren Nachfolger. Das bedeutet, dass zu jedem $a_n \geq a$, das von a verschieden ist, ein a_{n+1} existiert, das sowohl von a_n als auch von a verschieden ist und für welches $a_n \geq a_{n+1} \geq a$ gilt. Wir nehmen jetzt ein von a verschiedenes $a_1 \geq a$ an (das ist aufgrund der Bedingung 2 möglich) und bilden davon ausgehend die unendliche Folge

$$a_1 \geq a_2 \geq ... \geq a_n \geq a_{n+1} \geq ... \geq a$$

verschiedener Zahlen. Die Existenz einer solchen Folge widerspricht jedoch der Bedingung 4. Demzufolge existiert ein unmittelbarer Nachfolger von a. Seine Eindeutigkeit lässt sich mit Hilfe der Dichotomie ähnlich herleiten, wie dies in a) und b) geschah.

9. Gültig bleiben die Transitivität (3.), die Unbeschränktheit der Menge der Zahlen (5.), die Eigenschaft 4. und die Existenz des unmittelbaren Vorgängers (6.). Die Dichotomie wird durch die Trichotomie (entweder gilt $a > b$ oder $b > a$ oder $a = b$) ersetzt.
Die Reflexivität (1.) gilt nicht mehr, da $a > a$ immer falsch ist.
Was schließlich die Bedingung 2. betrifft, so bleibt sie formal in Kraft, denn streng genommen lautet diese Aussage in unserem Fall: Für beliebige natürliche Zahlen a und b folgt aus $a > b$ und $b > a$ die Beziehung $a = b$.

Nehmen wir an, diese Behauptung sei falsch. Dann müssen solche Zahlen a und b gefunden werden, für die gleichzeitig $a > b$, $b > a$ und $a \neq b$ gilt. Das ist aber unmöglich. Dieser Widerspruch beweist die Richtigkeit unserer Aussage.

10. Eine Menge beliebiger Objekte sei durch eine Relation $\succ$ geordnet, welche die Bedingungen 1. bis 7. erfüllt. Wie schon bewiesen, enthält sie dann ein Minimalelement, das wir mit a_0 bezeichnen wollen.
Aus den Ergebnissen der Aufgabe 8 folgt, dass jedes Element einen unmittelbaren Nachfolger hat. Wir bezeichnen das unmittelbar auf a_0 folgende Element mit a_1, das unmittelbar auf a_1 folgende Element mit a_2 usw. Als Ergebnis erhalten wir die Folge

$$a_0, a_1, a_2, ... \tag{23}$$

in welcher für jedes n die Relation $a_{n+1} \succ a_n$ gilt. Aufgrund der Reflexivität und Transitivität der Relation folgt hieraus, dass $a_i \succ a_j$ dann und nur dann gilt, wenn $i \geq j$ ist.

Es muss noch gezeigt werden, dass die Folge (23) tatsächlich alle von uns betrachteten Objekte umfasst. Das lässt sich mittels einer scharfsinnigen Überlegung durch vollständige Induktion bewerkstelligen.
Angenommen, b_0 gehöre der Folge (23) nicht an. Die Existenz von b_0 werten wir als ersten Schritt unserer Induktionsüberlegung. Es seien schon n Schritte durchgeführt werden, in deren Ergebnis wir ein Element b_{n-1} erhalten haben mögen. Für $b_{n-1} = a_0$ können wir unseren Prozess als beendet ansehen.
Für $b_{n-1} \neq a_0$ jedoch hat das Element b_{n-1} einen unmittelbaren Vorgänger, welcher mit b_n bezeichnet werde. Als Ergebnis erhalten wir eine Folge verschiedener Elemente

$$b_0 \succ b_1 \succ b_2 \succ ... \succ b_n \succ ...$$

Aufgrund der Bedingung 4. muss diese Folge ein letztes Glied haben. Nun kann aber nach dem Bildungsprinzip dieser Folge ihr letztes Glied nur a_0 sein. Um etwas Bestimmtes vor Augen zu haben, sei $b_n = a_0$.
Es ist leicht nachzuprüfen, dass dann, wenn a ein unmittelbarer Vorgänger von b ist, b unmittelbar auf a folgt. Das bedeutet

$$b_{n-1} = a_1, \quad b_{n-2} = a_2, \quad ..., \quad b_0 = a_n$$

Letzteres besagt, dass b_0 der Folge (23) angehört. Das aber widerspricht unserer Annahme. Demnach enthält die Folge (23) alle von uns untersuchten Objekte.

11. Es sei a eine Zahl. Jede Folge verschiedener Zahlen $a_0 = a, a_1, a_2, ..., a_n$, für welche

$$a_0 \succ a_1 \succ a_2 \succ ... \succ a_n \tag{24}$$

gilt und in welcher a_n im Sinne der Relation $\succ$ minimal ist, nennen wir eine Kette von Vorgängern von a_0; die Zahl n heißt dabei die Länge dieser Kette.

Wir zeigen zunächst, dass unter denjenigen Bedingungen, denen die Relation $\succ$ genügt, keine konkrete Zahl beliebig lange Ketten von Vorgängern haben kann.

Es sei a eine Zahl, $b_1, b_2, ..., b_k$ seien ihre unmittelbaren Vorgänger. Geht a_1 nicht unmittelbar der Zahl a_0 voran, dann können wir aufgrund von Bedingung 9. eine unmittelbar vor a liegende Zahl in die Kette (24) einfügen. Falls es also beliebig lange Ketten von Vorgängern von a gäbe, könnten auch solche beliebig lange Ketten gefunden werden, welche bei Zahlen beginnen, die a unmittelbar vorangehen. Im folgenden werden wir ausschließlich solche Ketten betrachten.

Jede Kette von Vorgängern von a ist genau um 1 länger als eine Kette von Vorgängern einer der unmittelbaren Vorgänger von a. Wenn jede dieser Zahlen Vorgängerketten beschränkter Länge hätte, dann könnte a selbst keine beliebig langen Ketten von Vorgängern haben.
Das bedeutet, dass unter unserer Annahme wenigstens eine der Zahlen, welche a_0 unmittelbar vorangehen, beliebig lange Vorgängerketten hat. Wir bezeichnen diese Zahl mit a_1 und wiederholen in Anwendung darauf alle soeben durchgeführten Überlegungen. Dadurch erhalten wir eine Zahl a_2, die unmittelbarer Vorgänger von a_1 ist und beliebig lange Vorgängerketten hat. Wiederholen wir dieses Verfahren, so kommen wir zu einer Folge

$$a_0 \succ a_1 \succ a_2 \succ ...$$

die der Bedingung 4. zufolge früher oder später abbrechen muss.
Das bedeutet, dass die Folge ein Glied enthält, auf welches unsere Überlegungen nicht mehr anwendbar sind. Wir haben aber die Anwendbarkeit der Überlegungen für jedes folgende Glied der Folge bereits nachgewiesen. Dieser Widerspruch zeigt, dass überhaupt keine Zahl beliebig lange Ketten von Vorgängern haben kann.

Demzufolge kann man unter den Ketten von Vorgängern jeder Zahl a eine längste auswählen. Wir bezeichnen ihre Länge mit $n(a)$. Ist b unmittelbarer Vorgänger von a, dann ist offensichtlich $n(b) = n(a) - 1$, und für alle minimalen a gilt $n(a) = 0$.

Schließlich sei $A(a)$ eine von a abhängige Aussage. Mit $B(n)$ wollen wir die folgende Aussage bezeichnen: $A(a)$ gilt für alle Zahlen a, für welche $n(a) = n$ ist. Wie leicht zu erkennen ist, stimmt dann die neue Formulierung des Induktionsprinzips für die Aussage $A(a)$ mit der Formulierung dieses Prinzips für die Aussage $B(n)$ überein.

12. a) Zu beliebigen geraden Zahlen a und b existieren immer gerade Zahlen q und r derart, dass

$$a = bq + r \qquad (0 \leq r < 2b) \tag{25}$$

gilt. Dabei sind die Zahlen q und r eindeutig bestimmt.

Beweis. Nach Satz 7 existieren solche q_0 und r_0, dass

$$a = bq_0 + r_0 \qquad (0 \leq r_0 \leq q_0)$$

erfüllt ist. Die Zahl r_0 muss nach Satz 6 gerade sein. Ist q_0 ebenfalls gerade, so können wir $q = q_0$ und $r = r_0$, setzen. Ist jedoch die Zahl q_0 ungerade, dann setzen wir $q = q_0 - 1$ (offenbar ist dieses q gerade) und $r = r_0 + b$. In beiden Fällen erhalten wir die Beziehung (25).

Nehmen wir an, es gäbe außer (25) noch eine andere Darstellung

$$a = bq' + r' \qquad (0 \leq r' < 2b)$$

mit geraden Zahlen q' und r'. Dann erhalten wir

$$b(q' - q) = r - r'$$

Wegen $0 \leq |r - r'| < 2b$ muss $|q' - q| < 2$ sein. Nun ist aber $q' - q$ eine gerade Zahl. Das bedeutet $q' - q = 0$, und hieraus folgt das Gewünschte.

13. Es sei p der kleinste Primteiler der Zahl a. Daraus folgt $a = pb$. Jeder Primteiler q der Zahl b ist außerdem auch Teiler von a. Daher ist $q \geq p$, also auch $b \geq p$, hieraus folgt $a \geq p^2$ und schließlich $p \leq \sqrt{a}$.

14. Die Bedingung ist notwendig. Es sei $b|a$. Aus Satz 13 folgt, dass jeder Primteiler von b auch Primteiler von a ist. Daher hat b die Form

$$p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$$

wobei $0 \leq \beta_1$, $0 \leq \beta_2$, ..., $0 \leq \beta_k$ ist. Angenommen, es sei $\beta_1 > \alpha_1$. Da

$$\frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}} = \frac{p_1^{\alpha_2} ... p_k^{\alpha_k}}{p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} ... p_k^{\beta_k}}$$

eine ganze Zahl ist, muss der Zähler dieses Bruches durch den Nenner, also erst recht durch die Zahl $p_1^{\beta_1 - \alpha_1}$ teilbar sein. Dann müsste nach Satz 13 aber wenigstens eine der Zahlen $p_2, ..., p_n$ durch p_1 teilbar sein, was unmöglich ist. Also ist $\beta_1 \leq \alpha_1$.
Da die Nummerierung der Primteiler von a beliebig ist, haben wir damit bewiesen, dass $\beta_2 \leq \alpha_2, ..., \beta_k = \alpha_k$ gilt. Die Notwendigkeit ist also bewiesen.
Um zu zeigen, dass die Bedingung hinreichend ist, bemerken wir, dass

$$a = bp_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} ... p_k^{\alpha_k - \beta_k}$$

gilt, wenn b die angegebene Form hat.

15. Es sei $p_1, p_2, ..., p_k$ die vollständige Liste aller Primzahlen, die wenigstens in einer der kanonischen Zerlegungen von a und b vorkommen. Wir setzen

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} \qquad , \qquad b = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$$

(Wenn a nicht durch p_i teilbar ist, gilt $\alpha_i = 0$; ist b nicht durch p_i teilbar, so ist $\beta_i = 0$.) Es sei γ_i die größte der Zahlen α_i und β_i für $i = 1, 2, ..., k$ und δ_i die kleinste dieser Zahlen. Dann ist aufgrund des bei der Lösung von Aufgabe 13 Gesagten der größte gemeinsame Teiler von a und b die Zahl

$$p_1^{\delta_1} p_2^{\delta_2} ... p_k^{\delta_k}$$

und ihr kleinstes gemeinsames Vielfache die Zahl

$$p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$$

16. Wie schon festgestellt wurde, muss jeder Teiler der Zahl a mit der kanonischen Zerlegung $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ die Form (26) haben, wobei β_1 die $\alpha + 1$ Werte $0, 1, 2, ..., \alpha_1$ und β_2 die entsprechenden $\alpha_2 + 1$ Werte haben kann, usw.
Da beliebige Kombinationen dieser Werte möglich sind und uns alle Teiler von a liefern, wobei jeder Teiler genau einmal auftritt (wenn einer der Teiler mehrfach vorkäme, so würde das bedeuten, dass für ihn mehrere kanonische Zerlegungen existieren), ist die Anzahl der Teiler von a gleich

$$(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$$

17. Es sei $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ die kanonische Zerlegung von a. Offen bar kann man $p_1 = 2$, $\alpha_1 \geq 2$ und $p_2 = 3$, $\alpha_2 \geq 1$ annehmen. Außerdem ist

$$(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1) = 14$$

Hieraus ergibt sich $k = 2$, $\alpha_1 + 1 = 7$ und $\alpha_2 + 1 = 2$, also $a = 2^6 \cdot 3 = 192$.

18. Es ist

$$\tau(a^2) = \tau(p_1^{2\alpha_1} p_2^{2\alpha_2}) = (2\alpha_1 + 1)(2\alpha_2 + 1) = 81$$

so dass $(2\alpha_1+1)(2\alpha_2+1)$ eine Zerlegung der Zahl 81 in zwei Faktoren ist. Da die Nummerierung der Primteiler von a von uns abhängt, können wir uns auf die Untersuchung folgender Möglichkeiten beschränken;

$$\begin{aligned} 2\alpha_1 + 1 = 1 \quad &, \quad 2\alpha_2 + 1 = 81 \\ 2\alpha_1 + 1 = 3 \quad &, \quad 2\alpha_2 + 1 = 27 \\ 2\alpha_1 + 1 = 9 \quad &, \quad 2\alpha_2 + 1 = 9 \end{aligned}$$

Im ersten dieser Fälle ist $\alpha_1 = 0$, im Widerspruch dazu, dass α_1 positiv sein soll. Die restlichen Fälle liefern

$$\alpha_1 = 1, \quad \alpha_2 = 13, \qquad \alpha_1 = 4, \quad \alpha_2 = 4$$

Das bedeutet entweder

$$\tau(a^3) = \tau(p_1^{3\alpha_1} p_2^{3\alpha_1}) = \tau(p_1^3 p_2^{39}) = (3 + 1)(39 + 1) = 160$$

oder

$$\tau(a^3) = \tau(p_1^{3\alpha_1} p_2^{3\alpha_1}) = \tau(p_1^{12} p_2^{12}) = 13 \cdot 13 = 169$$

19. Es sei $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ die kanonische Zerlegung der Zahl a. Die Voraussetzung der Aufgabe liefert

$$p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k} = 2(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)$$

oder

$$\frac{p_1^{\alpha_1}}{\alpha_1+1}\frac{p_2^{\alpha_2}}{\alpha_2+1}...\frac{p_k^{\alpha_k}}{\alpha_k+1} = 2 \tag{27}$$

Nun ist

$$\frac{2^1}{1+1} = 1 < \frac{2^2}{2+1} < \frac{2^3}{3+1} = 2 < \frac{2^\alpha}{\alpha+1}, \qquad (\alpha \geq 4)$$
$$1 < \frac{3^1}{1+1} < 2 < \frac{3^\alpha}{\alpha+1}, \qquad (\alpha \geq 2)$$
$$2 < \frac{p^\alpha}{\alpha+1}, \qquad (p \geq 5, \alpha \geq 1)$$

Daher ist in (27) jeder Bruch auf der linken Seite nicht kleiner als 1, also kann keiner der Brüche größer als 2 sein. Das bedeutet, dass auf der linken Seite nur Brüche stehen können, die unter den Brüchen

$$\frac{2^1}{1+1}, \frac{2^2}{2+1}, \frac{2^3}{3+1}, \frac{3^1}{1+1}$$

vorkommen. Ihr Produkt muss 2 sein. Das ist jedoch nur in zwei Fällen möglich: wenn in (27) nur der Bruch $\frac{2^3}{3+1}$ steht oder wenn dort die beiden Brüche $\frac{2^2}{2+1}$ und $\frac{3^1}{1+1}$ auftreten. Diesen beiden Fällen entsprechen die beiden Lösungen der Aufgabe, nämlich 8 und 12.

20. Für die geradzahlige Teilbarkeit gibt es keine den Sätzen 11 bis 14 ähnlichen Sätze. Die Zahlen 30 und 42 sind nämlich "gerade Primzahlen". Ihr kleinstes gemeinsames gerades Vielfaches ist 420, aber ihr Produkt 1260.

Ferner ist $60 = 6 \cdot 10$ geradzahlig teilbar durch die "gerade Primzahl" 30, die Zahlen 6 und 30 sind geradzahlig teilerfremd, aber 10 ist durch 30 nicht geradzahlig teilbar.
Schließlich sind $60 = 6 \cdot 10 = 30 \cdot 2$ zwei verschiedene Zerlegungen der Zahl 60 in "gerade Primfaktoren".

21. a) Hinsichtlich der Division durch 8 ist 116 restgleich mit 4 und 17 mit 1. Daher ist A restgleich mit $5^{21} = (5^2)^{10} \cdot 5$.
Nun ist aber $5^2 = 25$ hinsichtlich der Division durch 8 restgleich mit 1. Folglich liefert A bei der Division durch 8 den Rest 5.

b) Die Zahl 14 ist hinsichtlich der Division durch 17 restgleich mit -3. Daher ist A restgleich mit $-3)^{256} = 3^{256} = (3^3)^{85} \cdot 3$. Nun können wir 3^3 durch die restgleiche Zahl 10 ersetzen, und es ist $10^{85} \cdot 3 = (10^2)^{42} \cdot 30$. Ferner ist 10^2 hinsichtlich der Division durch 17 restgleich mit -2 und 2^4 mit -1.
Das heißt, A ist restgleich mit $(-2)^{42} \cdot 30 = 2^{42} \cdot 30 = (2^4)^{10} \cdot 4 \cdot 30 = (-1)^{10} \cdot 4 \cdot 30 = 120$, und diese Zahl liefert bei Division durch 17 den Rest 1.

22. a) Es sei n_1 der Rest von n, bei Division durch 6. Dann kann n_1 die Werte 0, 1,

2, 3, 4, 5 annehmen, und $n_1^3 + 11n_1$ ist hinsichtlich der Division durch 6 restgleich mit $n^3 + 11n$.
Wir haben also die Teilbarkeit der Zahlen 0, 12, 30, 60, 108 und. 180 durch 6 zu untersuchen. Alle diese Zahlen sind aber durch 6 teilbar.

b) Für $n \geq 2$ erhalten wir (unter Benutzung des binomischen Satzes)

$$\begin{aligned} 4^n + 15^n - 1 &= (3+1)^n + 15n - 1 \\ &= 3^n + 3^{n-1}\binom{n}{1} + ... + 3^2\binom{n}{n-2} + 3\binom{n}{n-1} + 1 + 15n - 1 \\ &= 9\left(3^{n-2} + 3^{n-3}\binom{n}{1} + ... + \binom{n}{n-2}\right) + 18n \end{aligned}$$

und offensichtlich sind beide Summanden durch 9 teilbar.
Für $n = 1$ erhalten wir $4^1 + 15 \cdot 1 - 1 = 18$.

c) Der Beweis wird mittels vollständiger Induktion geführt.
Für $n = 0$ haben wir

$$10^{3^0} - 1 = 10^1 - 1 = 9 \qquad \text{und} \qquad 3^{0-2} = 9$$

und die Behauptung ist richtig.
Nun gelte $3^{n+2} | (10^{3^n} - 1)$. Dann ist

$$10^{3^{n+1}} - 1 = (10^{3^n})^3 - 1^3 = (10^{3^n} - 1)(10^{2 \cdot 3^n} + 10^{3^n} + 1)$$

Nach Induktionsvoraussetzung ist der erste Faktor rechts durch 3^{n+2} teilbar. Im zweiten Faktor können wir die Zahl 10 durch 1 ersetzen, die hinsichtlich der Division durch 3 restgleich damit ist. Der zweite Faktor ist also durch 3 teilbar.
Folglich ist das Produkt durch $3^{n+3} = 3^{(n+1)+2}$ teilbar, was zu beweisen war.

d) Hinsichtlich der Division durch $a^2 - a + 1$ ist offensichtlich a^2 restgleich mit $a - 1$. Also ist $a^{2n+1} + (a-1)^{n+2}$ restgleich mit

$$a^{2n+1} + (a^2)^{n+2} = a^{2n+1} + a^{2n+4} = a^{2n+1}(1 + a^3) = a^{2n+1}(1+a)(1 - a + a^2)$$

was zu beweisen war.

23. Es sei $\sim$ eine Äquivalenzrelation über der Menge der Zahlen. Wir greifen eine beliebige Zahl a heraus und betrachten alle Zahlen, die zu a äquivalent sind. Sie sind aufgrund der Transitivität der Beziehung $\sim$ sämtlich zueinander äquivalent. Die Klasse aller dieser Zahlen bezeichnen wir mit K.

Jetzt betrachten wir eine beliebige Zahl b, die nicht zu K gehört.
Wäre $b \sim c$ und c eine Zahl aus K, so wäre auch $b \sim a$, was jedoch aufgrund der Wahl von b nicht sein kann. Das heißt, keine der Zahlen, die außerhalb von K liegen, ist einer der Zahlen in K äquivalent. Folglich ist K die Äquivalenzklasse, die a enthält.

Da die Zahl a völlig willkürlich gewählt war, zeigen unsere Betrachtungen, dass jede

Zahl einer bestimmten Äquivalenzklasse angehört. Damit ist die Behauptung bewiesen.

24. Offenbar gibt es unter den Zahlen $0, 1, 2, ..., m$ zwei Zahlen, die der gleichen Klasse angehören. Diese Zahlen seien k und l.
Dann ist also $k \sim l$. Es kann auch mehrere solcher Zahlenpaare in einer Klasse geben. Wir wählen darunter dasjenige Paar aus, für das der Wert $|k-l|$ am größten ist. Wegen $-l \sim -l$ erhalten wir nach Voraussetzung

$$k - l \sim l - l = 0$$

Ferner finden wir, dass auch für jedes ganze n

$$n(k - l) \sim 0$$

gilt. Schließlich gilt für jedes r

$$n(k - l) + r \sim r$$

d.h., aus $a \equiv b(\mathrm{mod}\, k - l)$ folgt $0 \sim b$. Somit enthalten die Äquivalenzklassen der Relation $\sim$ eine ganze Restklasse modulo m.
Dafür, dass es an Äquivalenzklassen der Relation $\sim$ gibt, ist notwendig, dass jede $\sim$-Äquivalenzklasse nicht mehr als eine Restklasse enthält und $k - l = m$ ist.

25. a) Beide Seiten einer Kongruenz und den Modul kann man durch eine (selbstverständlich von Null verschiedene) Zahl teilen. In der Tat bedeutet $ad \equiv bd(\mathrm{mod}\, md)$, dass

$$md|(ad - bd) = (a - b)d$$

d.h. $m|(a - b)$ gilt, woraus $a \equiv b(\mathrm{mod}\, m)$ folgt.

b) Beide Seiten einer Kongruenz kann man durch eine dem Modul teilerfremde Zahl dividieren. Sind nämlich d und m teilerfremd, so folgt aus

$$ad \equiv bd \pmod{m}$$

d.h. aus $m|(a-b)d$, aufgrund des Satzes 12, dass $m|(a-b)$ gilt, was zu beweisen war.

26. Wir nehmen an, es sei

$$1 \leq k < l \leq p - 1 \qquad , \qquad ka \equiv la \pmod{p}$$

Das bedeutet $p|(l - k)a$. Da a nicht durch p teilbar ist, muss $l - k$ durch p teilbar sein. Das kann aber wegen $0 < l - k < p$ nicht der Fall sein. Damit ist die Aussage bewiesen.

27. Die Bedingung ist notwendig. Es sei p eine Primzahl. Dann betrachten wir ein q mit $0 < q < p$. Unter den Zahlen $q, 2q, ..., (p - 1)q$ befindet sich genau eine, die bei Division durch p den Rest 1 liefert. Diese Zahl sei $\overline{q}q$:

$$\overline{q}q \equiv 1 \pmod{p}$$

Andererseits kann unter den Zahlen $\overline{q}, 2\overline{q}, ..., (p-1)\overline{q}$ ebenfalls nur eine Zahl sein, die bei Division durch p den Rest 1 liefert. Das ist aber die Zahl $\overline{q}q$, wie festgelegt. Nun klären wir, in welchen Fällen $\overline{q}$ gleich q ist. In allen diesen Fällen lässt sich die Kongruenz (28) in der Form

$$q^2 \equiv 1 \pmod{p}$$

oder, was das gleiche ist, in der Form

$$q^2 - 1 \equiv 0 \pmod{p}$$

darstellen. Das bedeutet

$$p|(q^2 - 1) = (q+1)(q-1)$$

Da p Primzahl ist, muss nach Satz 13 entweder $p|(q+1)$ oder $p|(q-1)$ gelten. Da die Zahl q zwischen 0 und p liegt, ist der erste Fall nur für $q = p-1$, der zweite nur für $q = 1$ möglich. Folglich kann man die übrigen Zahlen $2, ..., p-2$ so zu Paaren zusammenfassen, dass das aus den beiden Zahlen gebildete Produkt bei Division durch p den Rest 1 liefert.

Wir schreiben die Kongruenzen (28) für alle diese Paare auf und multiplizieren alle so erhaltenen $\frac{p+1}{2}$ Kongruenzen miteinander. Im Ergebnis dieser Multiplikation erhalten wir links das Produkt aller Zahlen von 1 bis $p-1$ (wobei die Faktoren 1 und $(p-1)$ doppelt aufgeführt sind) und rechts 1:

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

d.h.

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \equiv p-1 \pmod{p} \quad , \quad 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) + 1 \equiv 0 \pmod{p}$$

Die letzte Kongruenz bedeutet

$$p|(1 \cdot 2 \cdot ... \cdot (p-1) + 1)$$

was zu zeigen war.

Die Bedingung ist hinreichend. Ist p keine Primzahl, so kann sie in ein Produkt von zwei kleineren Zahlen zerlegt werden: $p = p_1 p_2$.
Im Fall $p_1 \neq p_2$ sind sowohl p_1 als auch p_2 Faktoren des Produktes $1 \cdot 2 \cdot ... \cdot (p-1)$, welches somit durch p_1 und p_2 und damit durch p teilbar ist.

Es sei jetzt $p_1 = p_2 = q$. Dann ist $p = q^2$ (d. h. gleich dem Quadrat einer Primzahl). Für $q > 2$ ist $p > 2q$, und in dem Produkt $1 \cdot 2 \cdot ... \cdot (p-1)$ sind q und $2q$ als Faktoren enthalten, so dass es durch q^2 und damit durch p teilbar ist.
In beiden Fällen kann $1 \cdot 2 \cdot ... \cdot (p-1) + 1$ nicht durch p teilbar sein. Für $p = 4$ schließlich ist $1 \cdot 2 \cdot 3 - 1 = 5$ nicht durch 4 teilbar.

28. Satz. Es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ die kanonische Zerlegung von m. Dann sind die Zahlen A und B hinsichtlich der Division durch m genau dann restgleich, wenn sie hinsichtlich der Division durch $p_1^{\alpha_1}$, durch $p_2^{\alpha_2}$, ..., durch $p_k^{\alpha_k}$ restgleich sind.

Beweis. Die Bedingung ist notwendig. Restgleichheit der Zahlen A und B hinsichtlich der Division durch m bedeutet $m|(A-B)$.
Um so mehr gilt $p_i^{\alpha_i}|(A-B)$ für $i=1,...,k$, d. h., die Zahlen A und B sind restgleich hinsichtlich der Division durch alle $p_i^{\alpha_i}$.

Die Bedingung ist hinreichend. Die Zahlen A und B seien hinsichtlich der Division durch jedes $p_i^{\alpha_i}$ restgleich. Wir bezeichnen den Rest von A und B bei Division durch $p_i^{\alpha_i}$ $(i=1,2,...,k)$ mit m. Es ist also

$$A \equiv r_i \pmod{p_i^{\alpha_i}} \tag{29}$$

Ferner setzen wir

$$\frac{m}{p_i^{\alpha_i}} = m_i \qquad (i=1,...,k)$$

und multiplizieren in der Kongruenz (29) beide Seiten und den Modul mit m_i:

$$Am_i \equiv m_i r_i \pmod{m}$$

Wenn wir alle so erhaltenen Kongruenzen addieren, gelangen wir zu

$$A(m_1 + m2 + ... + m_k) \equiv m_1 r_1 + m_2 r_2 + ... + m_k r_k \pmod{m} \tag{30}$$

Wegen der Restgleichheit von A und B hinsichtlich der Division durch $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ..., $p_k^{\alpha_k}$ erhalten wir auch

$$B(m_1 + m_2 + ... + m_k) \equiv m_1 r_1 + m_2 r_2 + ... + m_k r_k \pmod{m} \tag{31}$$

Subtrahieren wir (31) von (30), so ergibt sich

$$(A-B)(m_1 + m_2 + ... + m_k) \equiv 0 \pmod{m}$$

d. h.

$$m|(A-B)(m_1 + m_2 + ... + m_k)$$

Nun ist aber die Summe $m_1 + m_2 + ... + m_k$ zu m teilerfremd. Hätte sie nämlich mit m einen gemeinsamen Primteiler p, so wäre dieser in der kanonischen Zerlegung von m enthalten, d. h., er hätte die Form p_i. Dann wäre sowohl die gesamte Summe als auch jeder Summand außer einem - nämlich m_i - durch p_i teilbar. Das kann aber nicht sein.

Jetzt können wir den Satz 12 anwenden, welcher aussagt, dass $m|(A-B)$ gilt, d. h., die Zahlen A und B sind hinsichtlich der Division durch m restgleich.

29. a) Bei der Anwendung des Euklidischen Algorithmus auf die Zahlen a und b ergeben sich durch die Divisionen mit Rest Gleichungen, die wir hier systematisch aufschreiben:

$$\begin{aligned} a &= bq_0 + r_1 \\ b &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &... \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n \end{aligned} \tag{32}$$

Wir haben also $r_n|r_{n-1}$ erhalten. Wegen $r_{n-2} = r_{n-1}q_{n-1} + r_n$ ist $r_n|r - n - 2$. Setzen wir dieses Verfahren dem Gleichungssystem (32) entsprechend nach oben weiter fort, so erhalten wir schließlich $r_n|a$ und $r_n|b$, d.h., r_n ist ein gemeinsamer Teiler von a und b.

Es sei d ein beliebiger gemeinsamer Teiler von a und b. Wegen $a = bq_0 + r_1$ gilt also $d|r_1$. Gehen wir im Gleichungssystem (32) nach unten weiter, so erhalten wir nacheinander $d|r_2$, $d|r_3$, ..., $d|r_n$, d. h., r_n ist durch jeden gemeinsamen Teiler von a und b teilbar und ist also eben darum der größte gemeinsame Teiler dieser Zahlen.

b) Beweis durch vollständige Induktion: Wir setzen

$$A_0 = 0, \quad B_0 = 1, \quad A_1 = 1, \quad B_1 = -q_0$$

dann erhalten wir

$$r_0 = b = aA_0 + bB_0 \qquad \text{und} \qquad r_1 = aA_1 + bB_1$$

Nun sei

$$r_{k-1} = A_{k-1}a + b_{k-1}b \qquad , \qquad r_k = A_k a + B_k b$$

Dann gilt aber

$$r_{k+1} = r_{k-1} - r_k q_{k+1} = (A_{k-1} - q_{k+1}A_k)a + (B_{k-1} - q_{k+1}B_k)b$$

und wir brauchen nur noch

$$A_{k-1} - q_{k+1}A_k = A_{k-1} \qquad , \qquad B_{k-1} - q_{k+1}B_k = B_{k-1}$$

zu setzen. Die Zahlen A_n und B_n sind die gesuchten Zahlen A und B.

30. Sind b und c zueinander teilerfremd, so kann man aufgrund des bisher Gesagten ganze Zahlen B und C finden, für die $bB + cC = 1$ oder, nach Multiplikation mit a,

$$abB + acC = a$$

gilt. Nach Voraussetzung gilt $c|ab$, offenbar ist $c|ac$, daher gilt auch $c|a$. Das Weitere ist leicht ersichtlich.

31. Wir beschränken uns auf die Betrachtung des Kriteriums für die Restgleichheit hinsichtlich der Division durch 8.
Eine beliebige natürliche Zahl A sei in der Form $1000a+b$ mit $0 \leq b < 1000$ dargestellt; b ist also höchstens eine dreistellige Zahl, sie liefert die letzten drei Ziffern der Zahl A. Es sei

$$F(A) = \begin{cases} b & \text{für } A \geq 1000 \\ \text{Rest von } A \text{ bei Division durch 8} & \text{für } 8 \leq A < 1000 \\ \text{nicht definiert} & \text{für } \leq A < 8 \end{cases}$$

32. Für diejenigen Zahlen, deren kanonische Zerlegung die Form $2^\alpha \cdot 5^\beta$ hat.

33. Die Bedingungen a) und b) sind automatisch erfüllt. Da die Zahlen 10 und 1

hinsichtlich der Division durch 3 restgleich sind, müssen auch die Zahlen A und $f(A)$ restgleich sein. Schließlich lässt sich durch einfaches Nachrechnen zeigen, dass $f(A) < A$ für $A \geq 3$ gilt.

34. a) $f(858773) = 38$, $f(38) = 11$, $f(11) = 2$.
b) $f(A) = 4444 \cdot 4 = 17776$, $f(l7776) = 28$, $f(28) = 10$, $f(10) = 1$.

35. Das Kriterium der Restgleichheit hinsichtlich der Division durch 9 ist dem betrachteten Kriterium der Restgleichheit hinsichtlich der Division durch 3 ähnlich.
Um ein Restgleichheitskriterium hinsichtlich der Division durch 11 zu erhalten, stellen wir die Zahl A in der Form

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + ... + 10^2a_1 + a_0$$

dar, wobei $0 \leq a_i < 100$ ist. Offensichtlich entspricht diese Darstellung der Zerlegung einer Zahl in zweistellige "Blöckchen" (von rechts nach links). Es sei

$$f(A) = \begin{cases} a_0 + a_1 + ... + a_n \text{für } A \geq 100 \\ \text{Rest von } A \text{ bei Division durch 11} & \text{für } 11 \leq A < 100 \\ \text{nicht definiert} & \text{für } \leq A < 11 \end{cases}$$

Es muss noch gezeigt werden, dass die Zahlen A und $f(A)$ hinsichtlich der Division durch 11 tatsächlich restgleich sind und außerdem $f(A) < A$ ist.

Ein anderes Restgleichheitskriterium hinsichtlich der Division durch 11 erhalten wir aufgrund der Darstellung der Zahl A in der Form

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

wobei wir die Tatsache benutzen, dass 10 hinsichtlich der Division durch 11 restgleich mit -1 und 100 restgleich mit 1 ist. Die Zahl A ist daher mit der Zahl

$$a_0 - a_1 + a_2 - a_3 + ... \pm a_n$$

restgleich, und die Formulierung des entsprechenden Restgleichheitskriteriums kostet keine Mühe.

Schließlich kann man die Zahl A, wenn man sie in dreistellige "Gruppen" zerlegt, darstellen als

$$10^{3n}a_n + 10^{3n-3}a_{n-1} + ... + 10^3a_1 + a_0$$

mit $0 \leq a_i < 1000$. Dann ist A hinsichtlich der Division durch 37 restgleich mit der Summe $a_0 + a_1 + a_2 + ... + a_n$ und hinsichtlich der Division durch 7, 11 und 13 mit der alternierenden Summe $a_0 - a_1 + a_2 - ... \pm a_n$.

36. Sind die Zahlen a und b restgleich, dann gilt $m|(a-b)$. Dabei sind nach Satz 6 die beiden Zahlen a und b entweder durch m teilbar oder nicht.
Hinsichtlich der Division durch 3 sind die Zahlen 4 und 5 teilbarkeitsgleich, aber nicht restgleich.

37. Aus der Teilbarkeitsgleichheit hinsichtlich der Division durch m möge die Restgleichheit folgen. Das bedeutet, dass alle nicht durch m teilbaren Zahlen hinsichtlich der Division durch m ein und denselben Rest liefern. Dieser Rest muss also gleich 1 sein, so dass $m = 2$ ist.

38. Die Relation der Teilbarkeitsgleichheit hinsichtlich der Division durch m ist offensichtlich reflexiv (jede Zahl ist teilbarkeitsgleich mit sich selbst), symmetrisch (ist a teilbarkeitsgleich mit b, so ist b teilbarkeitsgleich mit a) und transitiv (ist a teilbarkeitsgleich mit b und b teilbarkeitsgleich mit c, so ist auch a teilbarkeitsgleich mit c).
Folglich ist die Teilbarkeitsgleichheit eine Äquivalenzrelation. Dabei fallen alle durch m teilbaren Zahlen in die eine Klasse und alle nicht durch m teilbaren Zahlen in die andere.

39. Man stellt leicht fest, dass für $m > 2$ die Teilbarkeitsgleichheit von Summen nicht aus der Teilbarkeitsgleichheit der Summanden folgt.
Die Teilbarkeitsgleichheit von Produkten ergibt sich genau dann aus der Teilbarkeitsgleichheit ihrer Faktoren, wenn m Primzahl ist. Ist nämlich eines der Produkte durch eine Primzahl p teilbar, so muss nach Satz 13 wenigstens einer der Faktoren dieses Produktes durch dieses p teilbar sein. Dann ist aber der ihm teilbarkeitsgleiche Faktor des anderen Produktes, also das ganze Produkt, durch p teilbar.

Ist jedoch ein Produkt nicht durch p teilbar, dann kann auch das andere nicht durch p teilbar sein (weil sonst aufgrund unserer Überlegungen auch das erste Produkt durch p teilbar wäre.)
Ist p dagegen eine zusammengesetzte Zahl, so brauchen Produkte teilbarkeitsgleicher Faktoren nicht restgleich zu sein. Es genügt, $p = p_1 p_2$ ($p_1 \neq 1, p_2 \neq 1$) zu setzen. Dann sind die Zahlen 1 und p_1 sowie die Zahlen 1 und p_2 in Bezug auf p teilbarkeitsgleich, aber ihr Produkt ist es offenbar nicht.

40. Folgt unmittelbar aus Aufgabe 36a).

41. Die Bedingungen a) und b) sind offensichtlich erfüllt.
Ist ferner $a - b \geq 0$, dann ist offenbar $f(A) < A$. Ist aber $a - 2b < 0$, so braucht diese Ungleichung nicht zu gelten. Dabei wird der größte Wert von $|a - 2b|$ für $a = 0$ und $b = 9$ angenommen, und zwar ist dieser Wert gleich 18.
Folglich muss für $A \geq 19$ die Ungleichung $f(A) < A$ gelten. Für kleinere Werte ist die Gültigkeit dieser Ungleichung durch die Definition der Funktion f gewährleistet.

Schließlich ist $10a + b$ hinsichtlich 7 teilbarkeitsgleich mit $50a + 5b$ (denn die Zahlen 5 und 7 sind teilerfremd) und somit auch mit $50a + 5b - 7(7a + b) = a - 2b$.

42. Hinsichtlich der Division durch 7 liefert 15 den Rest 1, aber $1 - 2 \cdot 5 = -9$ den Rest 5.

43. Bedingung c). $f(A) < A$ bedeutet $a + 4b < 10a + b$, d. h., $3b < 9a$. Daher ist für $a \geq 4$ die notwendige Bedingung erfüllt.
Bedingung d). Offenbar ist $10a + b$ hinsichtlich der Division durch 13 teilbarkeitsgleich mit $40a + 4b$, und diese Zahl ist restgleich mit $a + 4b$.

44. Das Teilbarkeitskriterium führt nicht mehr zum Ziel, weil $f(39) = 39$ ist.

45. Angenommen, wir sollen ein Teilbarkeitskriterium für eine Zahl m konstruieren. Dazu suchen wir ein passendes s, das zu m teilerfremd und möglichst klein ist und für das $m|(10s+1)$ gilt (das war der Fall für $m = 7$, s war gleich 2) oder aber $m|(10s-1)$ gilt (für $m = 13$ war $s = 4$).
Im ersten Fall ist $A = 10a + b$ hinsichtlich m teilbarkeitsgleich mit

$$10as + bs = (10s + 1)a - a + bs$$

d. h. mit $a - bs$, im zweiten Fall mit

$$(10s - 1)a + a + bs$$

So ist die Zahl $10a + b$ hinsichtlich der Division durch

17 teilbarkeitsgleich mit $a - 5b$,
19 teilbarkeitsgleich mit $a + 2b$,
23 teilbarkeitsgleich mit $a + 7b$,
29 teilbarkeitsgleich mit $a - 3b$,
31 teilbarkeitsgleich mit $a + 3b$.

Es sei dem Leser überlassen diese Teilbarkeitskriterien exakt zu formulieren.

46. a) Da 100 hinsichtlich der Division durch 49 restgleich mit 2 ist, ist jede Zahl der Form

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + ... + 10^2a_1 + a_0 \qquad (0 \leq a_i < 100)$$

hinsichtlich der Division durch 49 restgleich mit

$$2^n a_n + 2^{n-1}a_{n-1} + ... + 2a_1 + a_0$$

b) $10a + b$ ist hinsichtlich der Division durch 49 teilbarkeitsgleich mit $a + 5b$.

47. Die Bedingungen a) und b) sind automatisch erfüllt. Die Bedingungen c) und d) sind erfüllt, weil der Übergang von A zu $f(A)$ dem Ersetzen bestimmter Zahlen durch ihre Reste (die kleiner als die Zahlen selbst und restgleich mit ihnen sind) bei Division durch A entspricht.

48. a) $r_2 = r_3 = ... = r_n = 0$, d.h. $r_k = 0$ $(k \geq 2)$;
b) $r_3 = r_4 = ... = r_n = 0$, d.h. $r_k = 0$ $(k \geq 3)$;
c) $r_1 = r_2 = ... = r_n = 1$, d.h. $r_k = 1$;
d) $r_1 = r_3 = ... = r_{2t-1} = -1$, $r_2 = r_4 = ... = r_{2t} = 1$, d.h. $r_k = (-1)^k$;
e) $r_{6t+1} = 3$, $r_{6t+2} = 2$, $r_{6t+3} = 6$, $r_{6t+4} = 4$, $r_{6t+5} = 5$, $r_{6t} = 1$.

49. Sei dem Leser überlassen.

50. Weder $2^4 - 2$ noch $2^3 - 1$ ist durch 4 teilbar.

51. Für $p|a$ gilt $p|a^p$, und der Satz ist bewiesen. Wenn jedoch a nicht durch p teilbar ist,

so ist a teilerfremd zu p, und wir können die in der Voraussetzung des Satzes enthaltene Kongruenz kürzen:

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

Zum Beweis dieser Kongruenz dividieren wir jede der Zahlen der Form ta ($t = 1, 2, ..., p-1$) durch p mit Rest: $ta = q_t p + r_t$. Das kann wie folgt geschrieben werden:

$$\begin{aligned} a &\equiv r_1 \pmod{p} \\ 2a &\equiv r_2 \pmod{p} \\ &... \\ (p-1)a &\equiv r_{p-1} \pmod{p} \end{aligned} \tag{33}$$

Aus dem Ergebnis der Aufgabe 26 folgt, dass unter den Zahlen r jede der Zahlen $1, 2, ..., p-1$ genau einmal vorkommt. Wenn wir alle Kongruenzen (33) multiplizieren, erhalten wir

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)a^{p-1} \equiv 1 \cdot 2 \cdot ... \cdot (p-1) \pmod{p}$$

Jetzt brauchen wir diese Kongruenzen nur durch $1 \cdot 2 \cdot ... \cdot (p-1)$ zu kürzen.

52. $\varphi(12) = \varphi(2^2 \cdot 3) = 2^{2-1}(3-1) = 4$,
$\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 2^{3-1}(3-1)(5-1) = 32$,
$\varphi(1000) = \varphi(2^3 \cdot 5^3) = 2^{3-1}5^{3-1}(5-1) = 400$.

53. Wir setzen m in der Form $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ an. Dann ist a)

$$p_1^{\alpha_1}(p_1-1)p_2^{\alpha_2}(p_2-1)...p_k^{\alpha_k}(p_k-1) = 10$$

Das links stehende Produkt muss durch 5 teilbar sein. Demnach ist entweder eine der Zahlen $p_1, p_2, ..., p_k$ gleich 5 (es sei also etwa $p_1 = 5$) oder eine der Differenzen $p_1 - 1$, $p_2 - 1$, ..., $p_k - 1$ durch 5 teilbar (dann sei etwa $5|(p_1 - 1)$).
Im ersten Fall gilt $p_1 - 1 = 4$; das kann aber nicht sein, da 10 nicht durch 4 teilbar ist. Der zweite Fall ist nur möglich für $p_1 = 11$, da p_1 eine Primzahl sein und somit $(p_1 - 1)|10$ gelten muss. Dann ist aber $\alpha_1 = 1$, und aus Satz 21 folgt

$$\varphi\left(\frac{m}{11}\right) = 1$$

d. h. entweder $\frac{m}{11} = 1$ oder $\frac{m}{11} = 2$. Schließlich ist also $m_1 = 11$, $m_2 = 22$.

b)

$$p_1^{\alpha_1}(p_1-1)p_2^{\alpha_2}(p_2-1)...p_k^{\alpha_k}(p_k-1) = 8$$

Ist m ungerade, so ist $\alpha_1 = \alpha_2 = ... = \alpha_k = 1$ (weil die rechte Seite dieser Ungleichung eine Potenz von 2 ist):

$$(p_1-1)(p_2-1)...(p_k-1) = 8$$

Das ist nur möglich für $k = 2, p_1 = 3, p_2 = 5$, d.h. für $m = 15$.

Jetzt sei m gerade, und zwar sei $p_1 = 2$. Dann ist offensichtlich wie früher $\alpha_1 = ... = \alpha_k = 1$, und wir erhalten

$$2^{\alpha-1}(p_2 - 1)...(p_k - 1) = 8$$

Offenbar ist $\alpha \leq 4$. Für $\alpha = 1$ ist der Fall dem betrachteten ähnlich: Die Ungleichung ist nur möglich für $k = 3$, $p_2 = 3$, $p_3 = 5$, d. h. für $m = 30$.
Für $\alpha = 2$ ist $k = 2$, $p_2 = 5$ und $m = 20$.
Für $\alpha = 3$ ist $k = 2$, $p_2 = 3$ und $m = 24$.
Für $\alpha = 4$ schließlich ist $k = 1$ und $m = 16$.

Als Lösung unserer Aufgabe ergibt sich also $m_1 = 15$, $m_2 = 30$, $m_3 = 20$, $m_4 = 24$, $m_5 = 16$.

54. Wir nehmen an, es wäre

$$p_1^{\alpha_1}(p_1 - 1)p_2^{\alpha_2}(p_2 - 1)...p_k^{\alpha_k}(p_k - 1) = 14$$

Jede der Zahlen $p_i - 1$ ist entweder eine Eins oder eine gerade Zahl und kann somit nicht 7 sein. Da sie nur um 1 kleiner als ein Primzahl ist, kann sie nicht gleich 14 sein. Demnach müsste eine der Zahlen $p_i^{\alpha_i - 1}$ die Zahl 7 sein. Dann wäre aber $p_i - 1 = 6$, und 14 ist nicht durch 6 teilbar.

55. Es sei $m = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$. Wir betrachten zunächst den Fall, dass m eine Potenz einer Primzahl ist: $m = p^{\alpha}$.
Eine beliebige Zahl ist aber dann und nur dann zu m teilerfremd, wenn sie nicht durch p teilbar ist. Nun gibt es aber unter den Zahlen $0, 1, 2, ..., m - 1$ insgesamt m/p durch p teilbare Zahlen. Die übrigen sind zu p teilerfremd, und das sind

$$m - \frac{m}{p} = m\left(1 - \frac{1}{p}\right) = p^{\alpha}\left(1 - \frac{1}{p}\right) = p^{\alpha-1}(p - 1) = \varphi(m)$$

Zahlen.
An dieser Stelle wäre zu bemerken, dass a und m dann und nur dann teilerfremd sind, wenn der Rest von a, bei Division durch m zu a teilerfremd ist.

Nach unseren obigen Überlegungen ist die Anzahl der bei Division durch $p_i^{\alpha_i}$ zu $p_i^{\alpha_i}$ teilerfremden Reste gleich $\varphi(p_i^{\alpha_i})$.
Wie wir bei der Lösung der Aufgabe 40 festgestellt haben, folgt aus der Restgleichheit von Zahlen hinsichtlich der Division durch alle $p_i^{\alpha_i}$ ihre Restgleichheit hinsichtlich der Division durch m und umgekehrt. Außerdem ist eine Zahl genau dann zu m teilerfremd, wenn sie zu jeder der Zahlen $p_i^{\alpha_i}$ teilerfremd ist.
Folglich entspricht jeder Kombination von Resten bei Division durch die Zahlen $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ..., $p_k^{\alpha_k}$, die zu den entsprechenden Divisoren teilerfremd sind, genau ein zu m teilerfremder Rest bezüglich der Division durch m. Es bleibt zu bemerken, dass die Anzahl solcher Kombinationen von Resten gleich

$$\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})...\varphi(p_k^{\alpha_k}) = \varphi(m)$$

ist.

56. Sei dem Leser überlassen.

57. Offenbar ist $n^{13} - n = n(n^{12} - 1)$. Nun ist

$$n^{12} = n^{\varphi(13)} = n^{2\varphi(7)} = n^{3\varphi(5)} = n^{6\varphi(3)} = n^{12\varphi(2)}$$

Somit gilt für $p = 2, 3, 5, 7, 13$ entweder $p|n$ oder $p|(n^{12} - 1)$. Jetzt braucht nur noch auf Satz 16 verwiesen zu werden.

58. Der Leser möge die Aufgabe selbständig lösen.

59. Es sei d der größte gemeinsame Teiler der Zahlen a und b. Wenn c nicht durch d teilbar ist, dann ist die Gleichung

$$ax + by = c$$

nicht ganzzahlig lösbar; Ist jedoch c durch d teilbar, dann können beide Seiten der Gleichung durch d gekürzt werden, und wir kommen zu dem bereits betrachteten Fall.

60. Es seien A und B so beschaffen, dass $aA + bB = 1$ gilt. Wir setzen

$$x_t = cA + bt \qquad , \qquad y_t = c\frac{1 - aA}{b} - at$$

Dann ist

$$ax_t + by_t = a(cA + bt) + b\left(c\frac{1 - aA}{b} - at\right) = caA + abt + c(1 - aA) - abt = c$$

und (x_t, y_t) ist tatsächlich eine Lösung unserer Gleichung.

61. a) $x_t = 9 \cdot 5^5 + 7t = 28125 + 7t, \qquad y_t = 9\frac{1-5^6}{7} - 5t = -20088 - 5t.$

Da die absoluten Glieder und die Koeffizienten von t in den Formeln für x_t und y_t sozusagen "angenähert proportional" sind, können wir hoffen, eine Darstellung unserer Lösung in kleineren Zahlen zu erhalten. In der Tat können wir

$$x_t = 6 + 7(t + 4017) \qquad , \qquad y_t = -3 - 5(t + 4017)$$

schreiben oder, wenn wir $t + 4017 = t'$ setzen,

$$x_{t'} = 6 + 7t' \qquad , \qquad y_{t'} = -3 - 5t'$$

Wir bemerken, dass die in Aufgabe 60 angegebene Methode zum Lösen von Gleichungen in ganzen Zahlen es ermöglicht, zu kleineren Zahlen überzugehen. Allerdings erfordert diese Methode einige komplizierte Berechnungen.

b) Wir benutzen die Tatsache, dass 25 mod 13 zum Exponenten 2 gehört. Daher können wir schreiben:

$$x_t = 8 \cdot 25 + 13t = 200 + 13t$$
$$y_t = 8\frac{1 - 25^2}{13} - 25t = -384 - 25t$$

oder nach Vereinfachung

$$x_{t'} = 5 + 13t' \qquad , \qquad y_{t'} = -9 - 25t'$$

62. Die Bedingung c) ist automatisch erfüllt, die Bedingung (1) folgt aus Satz 25.

63.

m	17	19	27	29	31	49
k'	12 (oder 5)	2	19	3	28 (oder -3)	5

64. Sei dem Leser überlassen.

7 Literatur

deren Inhalt mit dem des vorliegenden Büchleins im Zusammenhang steht

DYNKIN, E. B., und W. A. USPENSKI, Mathematische Unterhaltungen, II: Aufgaben aus der Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1967.

GELFOND, A. O., Die Auflösung von Gleichungen in ganzen Zahlen, VEB Deutscher Verlag der Wissenschaften, Berlin 1968.

GOLOWINA, L. I., und I. M. JAGLOM, Induktion in der Geometrie (russ.), Nauka, Moskau 1967 (deutsche Übersetzung in Vorbereitung).

GÖRKE, L., Mengen, Relationen, Funktionen, VEB Volk und Wissen Verlag, Berlin 1968.

KALOUJNINE, L. A., Primzahlzerlegung, VEB Deutscher Verlag der Wissenschaften, Berlin 1971.

KLEINFELD, G., Übungen für Junge Mathematiker, Bd. 3: Ungleichungen, BSB B. G. Teubner Verlagsgesellschaft, Leipzig 1969.

KOROWKIN, P. P., Ungleichungen, VEB Deutscher Verlag der Wissenschaften, Berlin 1971.

KRBEK, F. VON, Über Zahlen und Überzahlen, BSB B. G. Teubner Verlagsgesellschaft, Leipzig 1969.

KUROSCH, A. G., Algebraische Gleichungen beliebigen Grades, VEB Deutscher Verlag der Wissenschaften, Berlin 1967.

KUROSCH, A. G., Vorlesungen über Allgemeine Algebra, B. G. Teubner Verlagsgesellschaft, Leipzig 1964.

LEHMANN, E., Übungen für Junge Mathematiker, Bd. 1: Zahlentheorie, B. G. Teubner Verlagsgesellschaft, Leipzig 1968.

MILLER, M., Rechenvorteile, B. G. Teubner Verlagsgesellschaft, Leipzig 1968.

SOMINSKI, I. S., Die Methode der vollständigen Induktion, VEB Deutscher Verlag der Wissenschaften, Berlin 1971.

TRACHTENBROT, B. A., Wieso können Automaten rechnen? VEB Deutscher Verlag der Wissenschaften, Berlin 1971.

WINOGRADOW, I. M., Elemente der Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1955.

WOROBJOW, N. N., Die Fibonaccischen Zahlen, VEB Deutscher Verlag der Wissenschaften, Berlin 1971.