E.B. Dynkin / W.A. Uspenski

Mathematische Unterhaltung II
Zahlentheorie

Übersetzung und Bearbeitung: Peter Friedel, Brigitte Mai
1966 Deutscher Verlag der Wissenschaften
MSB: Nr. 20
Abschrift und LaTex-Satz: 2021 https://mathematikalpha.de

Vorwort

Diesem Buch[1] liegen Arbeiten einer Sektion eines mathematischen Schulzirkels an der Moskauer Staatlichen M. W. Lomonossow-Universität aus den Studienjahren 1945/46 und 1946/47 zugrunde. Der eine der Autoren war Leiter dieser Sektion, der andere gehörte zu den Teilnehmern. Diese Sektion nannte sich Sektion allgemeinen Typs. Man beschäftigte sich darin mit Fragen aus verschiedenen Gebieten der Mathematik. Dabei war es grundsätzlich nicht das Ziel, den Teilnehmern neue Erkenntnisse zu vermitteln; es ging vielmehr darum, ihre Aktivität zu wecken und ihnen zu einem schöpferischen Verhältnis zur Mathematik zu verhelfen. Mehrere Disziplinen wurden dabei mit großem Erfolg behandelt.

In dem vorliegenden Buch sind Themen aus drei dieser Disziplinen - in gründlicher Überarbeitung und erweiterter Form - enthalten: Aufgaben über das Mehrfarbenproblem, Aufgaben aus der Zahlentheorie und Aufgaben aus der Wahrscheinlichkeitsrechnung, die mit den sogenannten Irrfahrten zusammenhängen.

Jedem dieser Themen waren mehrere aufeinanderfolgende Zusammenkünfte gewidmet. Im allgemeinen begannen diese mit einem Problem, das zu seiner Formulierung keiner neuen Begriffe bedurfte, mit dessen Lösung die Teilnehmer jedoch in den neuen Fragenkreis eingeführt wurden. Auch im weiteren Verlauf hingen die Vorträge des Leiters eng mit Aufgaben zusammen, die sich im Laufe der Unterhaltungen ergaben; manchmal wurden sie gleich an Ort und Stelle gelöst, meistens aber als Hausaufgabe bis zur nächsten Sitzung gestellt.

Ein bedeutender Teil des gesamten Stoffes war in Gruppen zusammenhängender Aufgaben angeordnet. Bei jeder Sitzung der Sektion war eine gewisse Zeit der Besprechung der Lösungen gewidmet, die dann anschließend dem Leiter als Ausgangspunkt für Verallgemeinerungen und Folgerungen dienten. In seinem Vortrag ging der Leiter auch auf schwierigere Fragen ein, die sich weniger in einzelne Aufgaben zergliedern ließen.

In dem vorliegenden Buch wurde die Form der durch Aufgaben unterbrochenen Darlegung beibehalten, wobei die Lösung der Aufgaben für das Folgende wesentlich ist.

Für die Lektüre der ersten beiden Abschnitte genügen die Kenntnisse der 7. Klasse der Oberschule, der dritte Abschnitt erfordert nicht viel mehr Kenntnisse. Das Buch ist in seiner Konzeption für Schüler der Oberklassen gedacht, kann jedoch auch für Arbeitsgemeinschaften von Studenten der ersten Semester benutzt werden.

Wir benutzen hier die Gelegenheit, A.N. Kolmogoroff unseren Dank auszusprechen; seine Ratschläge haben bedeutend zur Verbesserung dieses Buches beigetragen. Wir sagen auch E.E. Balasch Dank, dessen Aufgaben den Paragraphen 2 und 3 in Kap. IV des zweiten Abschnittes zugrunde liegen. Schließlich danken wir M.A. Neumark und I.M. Jaglom, die das Manuskript durchgesehen und eine Reihe von Hinweisen gegeben haben.

Abschließend möchten wir auch noch die sorgfältige Arbeit unseres Redakteurs A.S. Rywkin würdigen.

März 1952 E. Dynkin , W. Uspenski

[1] In der deutschen Ausgabe erscheinen die Abschnitte I, II, III des Originals als einzelne Bändchen (Anm. d. Red).

Hinweise zur Benutzung dieses Buches

Alle drei Abschnitte[2] sind voneinander unabhängig; daher kann der Leser sie in beliebiger Reihenfolge lesen; es ist dabei jedoch zu beachten, dass der erste Abschnitt der leichteste und der dritte der schwierigste ist.
Der Anhang zum ersten Abschnitt enthält die Lösung einer Aufgabe, die sich ihrem Charakter nach der Thematik dieses Abschnittes anschließt; dieser Anhang kann übrigens unabhängig vom ersten Abschnitt gelesen werden, da für sein Verständnis nichts weiter notwendig ist als die Definition der regulären Färbung.

Jeder Abschnitt ist einem bestimmten Thema gewidmet; die einzelnen Teile eines Abschnittes stehen untereinander in engem Zusammenhang. Daher muss jeder Abschnitt lückenlos von Anfang bis Ende durchgelesen werden.
Eine Ausnahme bilden nur die Kap. II und. IV des zweiten Abschnittes, die mit einem Sternchen versehen sind. Sie weichen etwas von der Grundlinie des Abschnittes ab und können bei der ersten Lektüre ohne Nachteil, für das Verständnis des Folgenden ausgelassen werden (das Kap. II ist im wesentlichen eine Ergänzung zu Kap. I und Kap. IV eine Ergänzung zu Kap. III).

Das Buch ist zur Aktivierung der Arbeit des Lesers gedacht.
Jeder Abschnitt enthält daher als organischen Bestandteil eine Reihe von Aufgaben. Die meisten Aufgaben sind in Gruppen zusammengefasst; jede derartige Gruppe ist in sich abgeschlossen.

Oft führen diese einzelnen Aufgaben, von denen eine auf der anderen aufbaut, den Leser zu einem abschließenden Resultat, das in der letzten Aufgabe einer jeden Gruppe enthalten ist (so beispielsweise die Aufgaben 21-27, 38-41 des ersten Abschnittes, die Aufgaben 28-32, 71-75 des zweiten Abschnittes u.a.m.).

Manchmal verdichten sich die Lösungen einer derartigen Gruppe nicht zu einem bestimmten Resultat, sondern führen eine neue Methode ein (beispielsweise die Aufgaben 11-14 des ersten Abschnittes). Schließlich sind einige Aufgaben bloße Übungen, mit deren Hilfe der Leser sich mit den neuen Begriffen vertraut machen kann (wie etwa die Aufgaben 1-8 des zweiten Abschnittes oder die Aufgaben 1-3 des dritten Abschnittes u.a.m.).

Es empfiehlt sich, die Formulierung aller Aufgaben einer vorliegenden Gruppe zu betrachten, bevor man die einzelnen Aufgaben löst. Wir empfehlen dem Leser, sich erst dann die am Ende des Buches angeführten Lösungen anzusehen, wenn er alle Aufgaben einer Gruppe gelöst hat; die von uns angegebenen Lösungen werden alle auf einem bestimmten Weg gewonnen, während der Leser durch selbständiges Überlegen eigene Beweismethoden finden kann.

Die Praxis der mathematischen Schulzirkel hat nämlich gezeigt, dass dabei manchmal einfachere und elegantere Lösungen gefunden werden, als sie vom Autor für die jeweilige Aufgabe gedacht waren.

[2] In der deutschen Ausgabe erscheinen die Abschnitte I, II, III des Originals als einzelne Bändchen (Anm. d. Red).

Die einzelnen Gruppen von Aufgaben unterscheiden sich nach ihrem Schwierigkeitsgrad in bedeutendem Maße voneinander. Nach den Erfahrungen der Arbeitsgemeinschaft an der Universität kann man jedoch im Mittel eine Woche als Arbeitszeit für eine bis zwei Gruppen von Aufgaben ansehen.

Wahrscheinlich wird dem Leser die selbständige Lösung sämtlicher Aufgaben einer Gruppe nicht in allen Fällen gelingen. Sollte er nach Lösung einer Aufgabe bei der zweiten auf Schwierigkeiten stoßen, die er nicht überwinden kann, so sei ihm empfohlen, die erste, bereits gelöste Aufgabe noch einmal zu überlesen.

Manchmal genügt dies bereits, um die Lösung zu finden, auch wenn es vorher beim besten Willen nicht gelingen wollte. Erweisen sich aber die Schwierigkeiten als unüberwindlich, so sehe man zunächst die Lösung dieser schwierigen Aufgabe nach und fahre erst dann mit der Lösung der folgenden Aufgaben fort.

Trotz der fundamentalen Rolle, welche die Aufgaben in diesem Buch spielen, ist es keineswegs eine Aufgabensammlung. Ebenso wichtig wie die Aufgaben ist der in dem Buch gebotene theoretische Stoff.

Das Verhältnis zwischen den Aufgaben und diesem Stoff ist in den einzelnen Kapiteln verschieden. Manchmal liegt das Wesentliche in den Voraussetzungen der Aufgaben, und die Rolle des Textes ist darauf beschränkt, neue Begriffe einzuführen und Folgerungen zu ziehen (wie beispielsweise im § 1 des ersten Abschnittes, im Kap. V des zweiten Abschnittes usw.). In anderen Fällen (wie im Kap. II des zweiten Abschnittes und dem gesamten dritten Abschnitt) liegt das Wesentliche im theoretischen Stoff, und die Aufgaben haben untergeordnete Bedeutung.
In allen Fällen stehen Text und Aufgaben in engem Zusammenhang und müssen in der Reihenfolge gelesen werden, in der sie im Buch angeführt sind.

Einen wesentlichen Teil dieses Buches bilden die Lösungen der Aufgaben, denen sich oft Folgerungen und Anmerkungen grundsätzlichen Charakters anschließen. Daher sollte man die Lösungen auch dann studieren, wenn man selbständig mit den Aufgaben fertig wurde.

Schließlich raten wir dem Leser, die Zeit für die Lösung von Aufgaben nicht zu scheuen. Jede Gruppe von Aufgaben, ja jede Aufgabe, die selbständig gelöst wurde, bereichert den Vorrat an Kenntnissen, die dem Leser zur Verfügung stehen. Ein selbständig erarbeiteter Gedanke ersetzt zehn Gedanken, die man mit fremden Worten erlernt hat.

Sogar dann, wenn der Versuch der Lösung einer Aufgabe nicht gelingt, ist die aufgewendete Zeit nicht umsonst: Nach gründlicher Durcharbeitung der Aufgabe wird man ihre Lösung mit ganz anderen Augen lesen; man wird die Ursachen seines Misserfolges suchen und verstehen, aus den Hilfsbetrachtungen jene grundsätzlichen Ideen herauszufinden, die zum Erfolg führen.

Inhaltsverzeichnis

1 Das Rechnen mit Restklassen (Restklassenarithmetik)

1.1 Das Rechnen mit Restklassen modulo m

[3] Bei der Addition zweier einstelliger Zahlen erhalten wir entweder eine einstellige Zahl, beispielsweise $1+4=5$, $7+2=9$, oder eine zweistellige, wie zum Beispiel $3+9=12$, $5+8=13$, $7+9=16$, $4+6=10$. Wir verabreden nun, bei zweistelligen Summen nur die letzte Ziffer zu berücksichtigen und

$$3+9=2, \qquad 5+8=3, \qquad 7+9=6, \qquad 4+6=0$$

zu schreiben.
Bei dieser neuen Definition der Addition ist die Summe zweier einstelliger Zahlen stets wieder eine einstellige Zahl.

Bei der Multiplikation zweier einstelliger Zahlen erhalten wir ebenfalls entweder eine einstellige Zahl, z.B. $2\cdot 3=6$, $1\cdot 8=8$, $3\cdot 3=9$, oder eine zweistellige Zahl: $6\cdot 7=42$, $7\cdot 8=56$, $9\cdot 9=81$. Für den Fall, dass das Produkt zweistellig ist, wollen wir wieder nur die letzte Stelle berücksichtigen und

$$6\cdot 7=2, \qquad 7\cdot 8=6, \qquad 9\cdot 9=1$$

schreiben.
Bei dieser neuen Definition der Multiplikation ist das Produkt zweier einstelliger Zahlen wieder eine einstellige Zahl.

Die hier eingeführten Rechenoperationen sind von denen, die wir gewöhnlich Addition und Multiplikation nennen und mit "$+$" und "$\cdot$" bezeichnen, verschieden; genau genommen müsste man deshalb für diese neuen Rechenoperationen neue Namen und Bezeichnungen einführen.
Es zeigt sich jedoch, dass alle Formeln der gewöhnlichen Algebra, die nur die Zeichen "$+$" und "$\cdot$" sowie eine beliebige Anzahl Klammern enthalten, auch für die neuen Rechenoperationen ihre Gültigkeit behalten.[4] Insbesondere gelten die Formeln

$$\begin{aligned} a+(b+c) &= (a+b)+c, \\ a+b &= b+a, \\ a(bc) &= (ab)c \\ a(b+c) &= ab+ac \end{aligned}$$

sowie die Formeln

$$\begin{aligned} (a+b)^2 &= a^2+2ab+b^2, \\ (a+b)^3 &= a^3+3a^2b+3ab^2+b^3, \\ (a+b)(c+d) &= ac+bc+ad+bd \end{aligned}$$

[3] In den Kapiteln 1 bis 4 bezeichnen wir mit m eine beliebige natürliche (ganze positive) Zahl größer als 1.

[4] Diese Formeln dürfen auch Potenzen mit ganzem positivem Exponenten enthalten, da eine Potenz mit ganzem positivem Exponenten nur eine Abkürzung für das Produkt mehrerer gleicher Faktoren ist.

und andere mehr. Daher kann der Gebrauch der Zeichen "+"und "·" nicht zu Missverständnissen führen.

Wir haben damit eine neue Arithmetik aufgebaut, die der Schularithmetik zwar ähnlich ist, sich aber doch von ihr unterscheidet. Diese neue Arithmetik wird uns bei der Lösung vieler Aufgaben der gewöhnlichen Arithmetik und Algebra behilflich sein.

Unsere neue Arithmetik nennen wir Arithmetik der Restklassen modulo 10 oder kurz Arithmetik modulo 10. Sie enthält nur die zehn Zahlen 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
Stellen wir einmal die Additions- und die Multiplikationstabellen dieser Arithmetik modulo 10 zusammen:

Additionstafel

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Multiplikationstafel

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Es sei hier noch erwähnt: Ersetzt man in irgendeiner Gleichung der gewöhnlichen Arithmetik, die außer Zahlen nur Plus-Zeichen, Mal-Zeichen und Klammern enthält, jede Zahl durch ihre letzte Ziffer, so erhält man eine Gleichung, die modulo 10 gilt. Beispielsweise erhalten wir aus den Identitäten

$$\begin{aligned}(18+15)(123+1341) &= 11\cdot 8\cdot 549,\\ 10+11+12+13+14+15 &= (10+15)3,\\ 2^{10}+151 &= 1175\end{aligned}$$

auf diese Art die modulo 10 geltenden Gleichungen[5]

$$\begin{aligned}(8+5)(3+1) &= 1\cdot 8\cdot 9,\\ 0+1+2+3+4+5 &= (0+5)3,\\ 2^{10}+1 &= 5\end{aligned}$$

1. Man zerlege die Zahl 0 in der Arithmetik modulo 10 auf alle möglichen Arten in zwei Faktoren.
2. Man schreibe ebenso alle möglichen Zerlegungen der 1 in Faktoren auf.

[5]Es versteht sich von selbst, dass der Exponent der Potenz nicht durch seine letzte Ziffer ersetzt wird. Er spielt in der Formel eine andere Rolle als die übrigen Zahlen; denn er gibt an, wie oft die Basis der Potenz mit sich selbst multipliziert werden muss.

3. Mit welcher Ziffer enden die Zahlen 6^{811}, 2^{1000}, 3^{999}?

In der Arithmetik modulo 7 gibt es sieben Zahlen:

$$0, 1, 2, 3, 4, 5, 6.$$

Addition und Multiplikation in der Arithmetik modulo 7 werden durch folgende Regeln bestimmt:
Um zwei Zahlen zu addieren, muss man ihre Summe im gewöhnlichen Sinn bilden und diese dann durch ihren Rest bei der Division durch 7 ersetzen; um zwei Zahlen zu multiplizieren, muss man ihr Produkt suchen und dieses dann durch den Rest bei der Division durch 7 ersetzen (daher unsere Bezeichnung "Restklassenarithmetik"; d. Red). Wir führen einige Beispiele an:

$$3 + 5 = 1, \quad 5 \cdot 3 = 1, \quad 4 + 6 = 3, \quad 3 \cdot 6 = 4, \quad 3 + 4 = 0, \quad 2 \cdot 6 = 5$$

4. Man stelle die Additions- und die Multiplikationstabelle der Arithmetik modulo 7 zusammen und schreibe alle Zerlegungen der Zahlen 0 und 1 heraus.

5. Man bestimme den Rest der Zahl 3^{100} bei der Division durch 7.

Die Arithmetik modulo 10 und die Arithmetik modulo 7, die wie bisher betrachtet haben, sind nur Spezialfälle der Arithmetik modulo m.
Es sei m eine beliebige positive ganze Zahl. Die Elemente der Arithmetik modulo m sind dann die Zahlen $0, 1, 2, ..., m - 1$ (d.h. die Zahlen des kleinsten nichtnegativen vollen Restsystems modulo m). Addition und Multiplikation dieser m Zahlen werden auf folgende Weise definiert:

Um zwei Zahlen zu addieren (bzw. zu multiplizieren), muss man den Rest der gewöhnlichen Summe (bzw. des Produktes) bei der Division durch m nehmen.

6. Man stelle die Additions- und Multiplikationstabellen der Arithmetik modulo 2, modulo 3, modulo 4 und modulo 9 zusammen.

7. Man berechne in der Arithmetik modulo 11

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10;\ 2^{10};\ 3^{10};\ 4^{10};\ 5^{10};\ 6^{10};\ 7^{10};\ 8^{10};\ 9^{10};\ 10^{10}$$

8. Man bestimme den Rest der Zahl 2^{1000} bei der Division durch 3, 5, 11, 13.

Die Subtraktion in der Arithmetik modulo m wird ähnlich wie in der gewöhnlichen Arithmetik als die der Addition entgegengesetzte Operation definiert. Eine Zahl x heißt Differenz der Zahlen b und a, d.h. $x = b - a$, wenn

$$a + x = b$$

gilt. So ist beispielsweise modulo 7: $2 - 5 = 4$, denn $5 + 4 = 2$ und $1 - 6 = 2$, denn $6 + 2 = 1$.

Die schnellste Methode zur Bestimmung der Differenz zweier Zahlen modulo m ist

folgende: Man berechne die gewöhnliche Differenz und addiere, falls sie negativ ist, m hinzu. So gilt beispielsweise modulo 7

$$1-5=-4=3 \qquad , \qquad 2-3=-1=6$$

Die Subtraktion ist stets ausführbar und gibt stets nur eine einzige Lösung. Dadurch ist die Benutzung des Zeichens „-“ für die Subtraktion gerechtfertigt, und jede in der gewöhnlichen Algebra gültige Gleichung, die nur die Zeichen „+“, „-“, „·“ sowie eine beliebige Anzahl Klammern enthält, behält auch modulo m ihre Gültigkeit. Insbesondere bleiben die Formeln[6]

$$-(-a)=a, \qquad -(a+b)=-a-b, \qquad -(a-b)=-a+b, \qquad a+(-b)=a-b$$

erhalten sowie die Formeln

$$\begin{aligned} a^2-b^2&=(a-b)(a+b),\\ (a-b)^2&=a^2-2ab+b^2,\\ (a-b)^3&=a^3-3a^2b+3ab^2-b^3 \end{aligned}$$

und andere mehr.

In der gewöhnlichen Arithmetik lässt sich die Restklassenarithmetik zur Probe bei Addition, Subtraktion oder Multiplikation verwenden. Dabei benutzt man die Tatsache, dass eine in der gewöhnlichen Arithmetik gültige Gleichung in eine modulo m gültige Gleichung umgewandelt werden kann, indem man jede Zahl dieser Gleichung durch ihren Rest bei der Division durch m ersetzt. Wir kontrollieren als Beispiel mit Hilfe der Arithmetik modulo 7 die (angebliche) Identität

$$74218 \cdot 21363 - 81835 = 1585446299 \tag{1}$$

Ersetzt man jede Zahl durch ihren Rest bei der Division durch 7, so erhält man

$$4 \cdot 6 - 5 = 1$$

Diese Gleichung ist modulo 7 nicht gültig. Das bedeutet, dass die Ausgangsgleichung falsch ist. Meistens werden zur Probe die Restklassen modulo 9 benutzt. Jede beliebige Zahl N ergibt nämlich bei Division durch 9 den gleichen Rest wie ihre Quersumme, was das Auffinden des Bestes wesentlich erleichtert.[7]

Wir weisen darauf hin, dass die Probe mit Hilfe der Arithmetik modulo m nicht immer den Fehler aufdeckt. Kontrollieren wir beispielsweise die falsche "Gleichung" (1) mit Hilfe der Arithmetik modulo 9, so erhalten wir die modulo 9 gültige Gleichung

$$4 \cdot 6 - 7 = 8$$

[6] Wie gewöhnlich bedeutet $-a$ die Zahl $0-a$. So gilt modulo 8 beispielsweise $-3=5$.

[7] Die Zahlen $10, 10^2, 10^3, \ldots$ ergeben bei Division durch 9 den Rest 1. Daher geben die Zahlen $N = a \cdot 10^n + b \cdot 10^{n-1} + \ldots + f$ und $a+b+\ldots+f$ bei Division durch 9 den gleichen Rest.

Um mit größerer Wahrscheinlichkeit einen Fehler zu finden, muss man die Probe gleichzeitig mit mehreren Restklassen modulo m durchführen, etwa mit Hilfe der Restklassen modulo 7 und modulo 9.

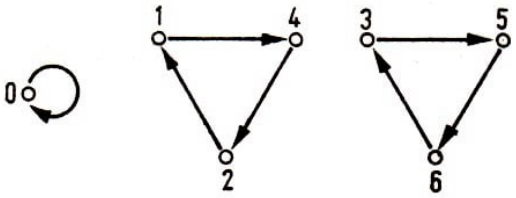
9. Man beweise, dass die Summe der dritten Potenzen aller Zahlen aus der Arithmetik modulo 1001 gleich Null ist.

10. a) Werden alle Zahlen modulo m (bei ungeradem m) in die gleiche ungerade Potenz k erhoben und dann addiert, so erhält man Null.
b) Man beweise, dass für alle ungeraden Zahlen m und k die Summe $1^k + 2^k + ... + (m-1)^k$ durch m teilbar ist.

1.2 Die Arithmetik der Restklassen modulo p

1.2.1 Multiplikationsschemata. Der (kleine) Fermatsche Satz

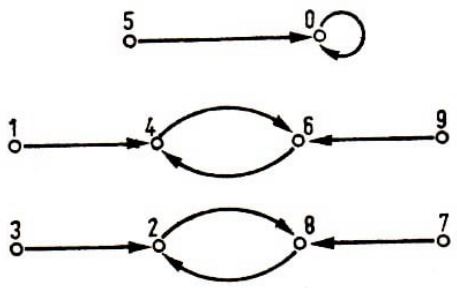
[8] Wir stellen die Zahlen $0, 1, 2, 3, 4, 5, 6$ aus der Arithmetik modulo 7 durch Punkte dar und deuten durch Pfeile an, in welche Zahl jede Zahl bei der Multiplikation mit 4 übergeht. Wir erhalten so das Schema in Abb. B.1.



B.1

[9]Dieses Schema kann man als Multiplikationstafel für die Zahl 4 in der Arithmetik modulo 7 benutzen. Daher nennen wir es das Schema der Multiplikation mit 4 in der Arithmetik modulo 7.

Genauso wird das Schema der Multiplikation mit 4 in der Arithmetik modulo 10 konstruiert (Abb. B.2). Eine Folge von n Zahlen, die in einem bestimmten Schema abgebildet sind, heißt Zyklus, wenn von jeder dieser Zahlen zur nachfolgenden und von der letzten zur ersten ein Pfeil gezogen werden kann. Die von uns konstruierten Schemata enthalten derartige Zyklen, und zwar:
Schema in Abb. B1: 0; 1, 4, 2; 3, 5, 6.
Schema in Abb. B2: 0; 4, 6; 2, 8.



B.2

[8]In den Kapiteln 1 bis 4 bedeutet p eine Primzahl, d.h. eine natürliche Zahl größer als 1, die außer 1 und sich selbst keine positiven Teiler hat.

[9]Da die Lage der Punkte, die den Zahlen 0, 1, 2, 3, 4, 5, 6 entsprechen, gleichgültig ist, haben wir sie derart verteilt, dass wir lange Pfeile vermeiden können.

Wir weisen auf einen wesentlichen Unterschied zwischen diesen Schemata hin: Im ersten kommt jede Zahl in einem bestimmten Zyklus vor (und zwar in genau einem); im zweiten kommen die Zahlen 1, 3, 5, 7, 9 in keinem Zyklus vor.

11. Man konstruiere die Schemata der Multiplikation mit 0, 1, 2, 3, 4, 5, 6 in der Arithmetik modulo 7, die Schemata der Multiplikation mit 2 und 5 in der Arithmetik modulo 10 und das Schema der Multiplikation mit 3 in der Arithmetik modulo 9.

12. Sind a und b Zahlen der Arithmetik modulo p und gilt $a \cdot b = 0$, so ist entweder a oder b gleich Null.

13. Es sei a eine beliebige Zahl aus der Arithmetik modulo p ($a \neq 0$). Man beweise, dass das Schema der Multiplikation mit a folgende Eigenschaften besitzt:
a) Zu keiner Zahl können zwei Pfeile führen;
b) zu jeder Zahl führt ein Pfeil.

14. Es seien a und b beliebige Zahlen aus der Arithmetik modulo p und $a \neq 0$. Unter Benutzung der vorhergehenden Aufgabe ist zu beweisen, dass modulo p genau eine Zahl x gefunden werden kann, die der Gleichung $ax = b$ genügt.

15. Es sei a eine beliebige Zahl aus der Arithmetik modulo 10. Man beweise, dass
a) das Schema der Multiplikation mit a in Zyklen zerfällt;
b) alle Zyklen (mit Ausnahme des Nullzyklus) die gleiche Länge haben.
Daraus ist abzuleiten, dass $a^{p-1} = 1$ ist.

16. Der kleine Fermatsche Satz. Ist p eine Primzahl und a teilerfremd zu p, so ist $a^{p-1} - 1$ durch p teilbar.

1.2.2 Die Division. Der Wilsonsche Satz

Die Division in der Arithmetik modulo m wird als die zur Multiplikation inverse (reziproke) Operation definiert.
Die Zahl x heißt Quotient der Division von b durch a (oder Verhältnis von b zu a), wenn $ax = b$ gilt.

Die Division braucht nicht ausführbar zu sein. Beispielsweise ist es in der Arithmetik modulo 10 nicht möglich, eine Zahl x zu finden, für die $4x = 5$ ist.
Andererseits braucht die Division, wenn sie ausführbar ist, nicht eindeutig ausführbar zu sein. So ist modulo 10 beispielsweise $4 \cdot 8 = 2$ und $4 \cdot 3 = 2$, so dass die Zahlen 8 und 3 in gleicher Weise als Quotienten bei der Division durch 4 bezeichnet werden können.

Aus der Aufgabe 14 folgt jedoch, dass in einer Arithmetik modulo p (p eine Primzahl) die Division durch jede beliebige Zahl a ($a \neq 0$) stets möglich und eindeutig ist)[10]

[10] Die Division einer Zahl $a \neq 0$ durch 0 ist auch in der Arithmetik modulo p unmöglich, da es keine Zahl x gibt, die der Gleichung $0x = a$ genügt. Es ist jedoch manchmal zweckmäßig, sich auf die Schreibweise $\frac{a}{0} = \infty$ zu einigen. Dabei muss man aber beachten, dass das Symbol ∞ keine Zahl ist und man dementsprechend mit ihm nicht wie mit einer Zahl operieren darf.

Auf Grund dieser wichtigen Tatsache bleibt jede Gleichung der gewöhnlichen Algebra, die nur die Zeichen $+$, -, $\cdot$, : (oder Bruchstriche) enthält, auch modulo p richtig. Insbesondere behalten die fünf Formeln

$$\frac{a}{b} \cdot c = \frac{ac}{b}, \quad \frac{a}{b} : c = \frac{a}{bc}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

und andere mehr ihre Gültigkeit.

Unter Benutzung der Arithmetik modulo p kann man Rechenoperationen mit Brüchen ähnlich kontrollieren wie mit Hilfe der Arithmetik modulo m Rechenoperationen mit ganzen Zahlen. Um beispielsweise die (angebliche) Gleichung

$$\frac{5}{22} + \frac{3}{17} - \frac{4}{15} = \frac{739}{5610}$$

zu kontrollieren, wird in der Gleichung jede Zahl durch ihren Rest bei der Division durch eine Primzahl p ersetzt. Man erhält beispielsweise bei Division durch 7:[11]

$$\frac{5}{1} + \frac{3}{3} - \frac{4}{1} = \frac{4}{3}$$

Diese Gleichung ist modulo 7 falsch; folglich ist in dem Ausgangsbeispiel ein Fehler enthalten.

17. In der Arithmetik modulo 7, modulo 11 und modulo 13 sind Tabellen der reziproken Größen $\frac{1}{k}$ aufzustellen. Als Beispiel bringen wir die Tabelle der reziproken Größen (Kehrwerte) in der Arithmetik modulo 5:

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

Man zeige, dass in jeder Arithmetik modulo p nur die Elemente 1 und -1 zu sich selbst reziprok sind.

18. a) Man beweise, dass das Produkt aller von Null verschiedenen Elemente der Arithmetik modulo p gleich -1 ist.

b) (Der Wilsonsche Satz). Ist p eine Primzahl, so ist $(p-1)!+1$ durch p teilbar.[12]

19. (Die Umkehrung von Aufgabe 18b) Ist $(m-1)!+1$ durch m teilbar, so ist m eine Primzahl.

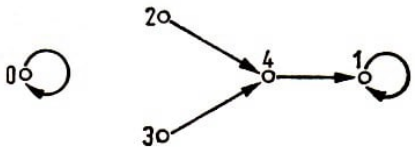
20. Wird jede Zahl einer Arithmetik modulo p in die k-te Potenz erhoben und werden alle diese Potenzen addiert, so erhält man als Resultat entweder 0 oder -1.

[11] Die Zahl p ist derart zu wählen, dass sie nicht als Faktor in einem der Nenner auftritt. Andernfalls würden wir eine Gleichung modulo p erhalten, die eine Division durch 0 enthielte.

[12] Dabei ist $n!$ die Abkürzung für das Produkt $1 \cdot 2 \cdot 3 \cdot ... \cdot n$ aller ganzen Zahlen von 1 bis n. Also ist $(p-1)! = 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)$.

1.3 Quadratwurzelziehen. Quadratische Gleichungen

Genau wie früher werden wir wieder die Zahlen der Arithmetik modulo p durch Punkte darstellen. Wir konstruieren ein Schema zum Quadrieren der Zahlen aus der Arithmetik modulo 5 (Abb. B.3).



B.3

21. Es sind Schemata zum Quadrieren in den Arithmetiken modulo 7, modulo 12 und modulo 24 zu konstruieren. (Dabei sind die Punkte in den Abbildungen so anzuordnen, dass die Schemata möglichst einfach werden.)

22. Man beweise, dass zu jedem Punkt (außer Punkt 0) in dem konstruierten Schema der Arithmetik modulo p entweder kein Pfeil oder zwei Pfeile führen.[13] Mit anderen Worten:
Man beweise, dass für $a \neq 0$ die Gleichung $x^2 = a$ in der Arithmetik modulo p entweder zwei verschiedene Lösungen oder keine Lösung hat.

23. Man beweise, dass sich aus genau $\frac{p+1}{2}$ Zahlen der Arithmetik modulo p die Quadratwurzeln ziehen lassen (und folglich aus den restlichen $\frac{p-1}{2}$ Zahlen nicht).

Wenn in den Schemata, die zur Lösung der Aufgabe 21 konstruiert werden sind (siehe die Abb. B.18 bis B.20), die Richtungen der Pfeile umgekehrt werden, so erhält man Schemata für das Quadratwurzelziehen in der Arithmetik modulo 7 bzw. modulo 12 bzw. modulo 24.

Aus allen Schemata ist ersichtlich, dass in der Arithmetik modulo m das Symbol $\sqrt{a}$ entweder 0 oder zwei oder vier oder mehr verschiedene Werte annehmen kann. Gemäß Aufgabe 22 gibt es jedoch modulo p nur zwei Möglichkeiten:
Entweder lässt sich $\sqrt{a}$ nicht ziehen, oder die Wurzel hat zwei verschiedene Werte. (Wir setzen dabei stets $a \neq 0$ voraus; $\sqrt{0}$ hat nur einen Wert, nämlich 0.)

24. a) Man beweise, dass sich in der Arithmetik modulo p die Quadratwurzel aus -1 ziehen lässt, wenn $p = 4k + 1$ ist, aber nicht, wenn $p = 4k + 3$ ist.
Hinweis. Man benutze die Aufgaben 15 und 18.

b) Man beweise, dass alle Primteiler der Zahl a^2+1 (bei beliebigem a) die Form $4k+1$ haben. Jede Primzahl der Form $4k + 1$ tritt bei Zerlegung von mindestens einer Zahl der Form $a^2 + 1$ in Primfaktoren auf.

25. Es ist die Formel für die Lösung in der Arithmetik modulo p der quadratischen Gleichung

$$ax^2 + bx + c = 0$$

(a, b und c sind Zahlen aus der Arithmetik modulo p, $a \neq 0$) abzuleiten. Unter Verwendung dieser Formel ist zu beweisen:

[13] In den Aufgaben 22-25 bezeichnet der Buchstabe p eine von 2 verschiedene Primzahl.

Besitzt $\sqrt{b^2-4ac}$ in der Arithmetik modulo p keine Lösung[14], so hat die Gleichung keine Wurzel;
ist $b^2-4ac \neq 0$, so besitzt die Gleichung genau eine Wurzel;
ist $b^2-4ac \neq 0$ und kann man $\sqrt{b^2-4ac}$ ziehen, so hat die Gleichung zwei verschiedene Wurzeln.

26. Man löse die quadratischen Gleichungen

$$5x^2+3x+1=0 \quad , \quad x^2+3x+4=0 \quad , \quad x^2-2x-3=0$$

in der Arithmetik modulo 7.

27. Jede quadratische Gleichung kann man auf die Form

$$x^2+cx+d=0$$

bringen, indem man sie durch den Koeffizienten des Gliedes mit dem höchsten Exponenten dividiert. Die Anzahl der verschiedenen quadratischen Gleichungen dieser Form in der Arithmetik modulo p ist p^2.
Es ist zu berechnen, wie viele von ihnen keine Wurzel, eine Wurzel oder zwei Wurzeln haben.

1.4 Kubikwurzelziehen. Primfaktoren von Zahlen der Form a^2+3

28. Man stelle das Schema der Kubikzahlen für die Arithmetik modulo 7, 11, 13 und 17 auf (vgl. Aufgabe 21).

Kehrt man die Richtung aller Pfeile in den Schemata, die in Aufgabe 28 konstruiert sind (siehe zur Lösung der Aufgabe 28 die Abb. B21 bis B.24), um, so erhält man Schemata für das Kubikwurzelziehen.
Aus den Schemata ist ersichtlich, dass in der Arithmetik modulo 11 und der Arithmetik modulo 17 die Kubikwurzel aus jeder beliebigen Zahl zu ziehen ist und nur einen Wert hat.

In der Arithmetik modulo 7 und der Arithmetik modulo 13 besitzt jedoch $\sqrt[3]{a}$ entweder drei verschiedene Werte, oder die Wurzel lässt sich nicht ziehen (eine Ausnahme bildet $a=0$; hier hat die Kubikwurzel nur die einzige Lösung 0).

29. Es sei p eine Primzahl der Form $3k+2$. [15] Man beweise, dass in der Arithmetik modulo p
a) $\sqrt[3]{1}$ nur einen Wert hat (nämlich 1) (hierbei ist die Aufgabe 15 zu benutzen);
b) $\sqrt[3]{a}$ für kein a mehr als einen Wert hat;
c) $\sqrt[3]{a}$ für jedes a existiert.

[14] Der Ausdruck b^2-4ac wird die Diskriminante der Gleichung $ax^2+bx+c=0$ genannt.
[15] Zahlen solcher Form sind beispielsweise $11=3\cdot 3+2$, $17=3\cdot 5+2$. Die Primzahlen 7 und 13 dagegen haben die Form $3k+1$.

30. Unter Benutzung der Identität

$$x^3 - 1 = (x-1)(x^2 + x + 1)$$

ist die Gleichung

$$x^3 - 1 = 0$$

zu lösen. Mit Hilfe der erhaltenen Formeln sind drei Werte für $\sqrt[3]{1}$ in der Arithmetik modulo 103 zu berechnen.

31. Es sei $p > 3$. Man beweise, dass $\sqrt{1}$ in der Arithmetik modulo p entweder drei verschiedene Werte oder nur einen Wert hat, je nachdem, ob $\sqrt{-3}$ existiert oder nicht.

32. Ist die Primzahl p Teiler einer Zahl der Form $a^2 + 3$, so ist p entweder gleich 2 oder 3, oder p hat die Form $3k + 1$.

1.5 Polynome und Gleichungen höheren Grades

Wir betrachten das Polynom

$$a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n \tag{1}$$

mit Koeffizienten aus der Arithmetik modulo p. Dabei setzen wir immer voraus, dass $a_0 \neq 0$ ist. In diesem Fall heißt n der Grad des Polynoms (1).
Eine Nullstelle des Polynoms

$$a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n \tag{1}$$

heißt Wurzel der Gleichung, das ist also eine Zahl x_0 mit

$$a_0 x_0^n + a_1 x_0^{n-1} + ... + a_{n-1} x_0 + a_n = 0 \tag{1}$$

In den vorhergehenden Abschnitten wurde gezeigt, dass Gleichungen zweiten Grades nicht mehr als zwei Wurzeln haben. Wir werden dieses Resultat auf Polynome beliebigen Grades ausdehnen.

33. Hat ein Polynom mehr Nullstellen, als sein Grad anzeigt, so sind alle Koeffizienten gleich Null.[16]

34. Gilt $x^k = 1$ für jedes $x \neq 0$, so ist k durch $p - 1$ teilbar.

35. Es seien $a \neq 0$ und $p \neq 2$. Man beweise, dass aus der Lösbarkeit von $\sqrt{a}$ in der Arithmetik modulo p die Gleichung $a^{\frac{p-1}{2}} = 1$ folgt und, falls sich $\sqrt{a}$ nicht lösen lässt, $a^{\frac{p-1}{2}} = -1$ ist.

36. Hat ein Polynom n-ten Grades n Nullstellen $x_1, x_2, ..., x_n$, so gilt

$$a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n = a_0 (x - x_1)(x - x_2)...(x - x_n)$$

[16] Genau genommen hat nach unserer Definition ein Polynom, dessen Koeffizienten alle 0 sind, überhaupt keinen Grad. Der eigentliche Sinn der Aufgabe ist: Ein Polynom kann nicht mehr Nullstellen haben, als sein Grad angibt. Diese Aussage gilt auch in der gewöhnlichen Arithmetik.

37. Man beweise, dass in der Arithmetik modulo p

$$(x-1)(x-2)...[x-(p-1)| = x^{p-1}-1$$

gilt. Daraus leite man den Satz von Wilson ab (Aufgabe 18b)).

2 m-adische und p-adische Zahlen

2.1 Division mehrstelliger Zahlen mit Hilfe der Arithmetik modulo 10

In der Grundschule lernt man vier Rechenarten für mehrstellige Zahlen: Addition, Subtraktion, Multiplikation und Division. Die Addition und die Multiplikation mehrstelliger Zahlen lassen sich vollständig auf die Addition und Multiplikation einstelliger Zahlen zurückführen:
Um zwei Zahlen zu addieren oder zu multiplizieren, muss man in bestimmter Reihenfolge Rechenoperationen mit den einzelnen Ziffern durchführen, wobei die Stellenwerte zu berücksichtigen sind.
Um beliebige mehrstellige Zahlen zu subtrahieren, genügt es, die Subtraktion im Bereiche von Zwanzig ausführen zu lassen.

Ganz anders bei der Division: Die allgemein übliche Methode des Dividierens ist ihrem Wesen nach nichts anderes als ein geordnetes System des Probierens.
Die einfachste Divisionsmethode wäre folgende: Man schätzt ab, wie groß der Quotient sein könnte, und multipliziert den vermuteten Quotienten mit dem Divisor. Falls dann das Produkt gleich dem Dividenden ist, ist die gefundene Lösung richtig. Ist das Produkt größer oder kleiner als der Dividend, so muss man den erratenen Quotienten entsprechend verkleinern bzw. vergrößern.
Nach endlich vielen Proben kommen wir dann zwangsläufig zur richtigen Lösung.

Falls der Quotient einstellig ist, fällt diese Methode mit der in der Schule gebräuchlichen zusammen. Ist der Quotient mehrstellig, so gestatten es die Schulregeln, die Aufgabe in einzelne Teile zu zerlegen, für die der Quotient einstellig ist und deren Lösung sich mit Hilfe des Abschätzens erhalten lässt.

Die Anwendung der Arithmetik modulo 10 gestattet es, auf andere Weise zu dividieren, indem man nämlich mit der letzten Ziffer des Dividenden und des Divisors ähnlich wie bei der Addition und der Multiplikation beginnt.
Wir stellen eine Tabelle der reziproken Größen der Arithmetik modulo 10 zusammen:

k	1	3	7	9
$\frac{1}{k}$	1	7	3	9

Die Zahlen, die in der gleichen Spalte dieser Tabelle stehen, ergeben bei der Multiplikation 1. Die Zahlen 2, 4, 5, 6, 8, 0 kommen in der Tabelle nicht vor; zu ihnen gibt es keine reziproken Größen.

Bei der Multiplikation der 5 mit irgendeiner Zahl erhalten wir beispielsweise entweder 5 oder 0, jedoch niemals l. Die Division ist in der Arithmetik modulo 10 nicht immer ausführbar, da 10 keine Primzahl ist.
Durch die Zahlen 1, 3, 7 und 9 kann jedoch immer dividiert werden. Um eine Zahl a durch eine dieser Zahlen zu dividieren, genügt es, a mit der reziproken Zahl zu multiplizieren.

Gehen wir zur Division mehrstelliger Zahlen über. Es ist bequem, die Erklärungen an irgendeinem Beispiel auszuführen.
Angenommen, es sei verlangt, 74646 durch 957 zu dividieren. Im Sinne des Rechnens in der Arithmetik modulo 10 dividieren wir die letzte Ziffer des Dividenden durch die letzte Ziffer des Divisors:

$$6 : 7 = 6 \cdot 3 = 8$$

Wir erhalten die letzte Ziffer des Quotienten. Nun multiplizieren wir diese Ziffer mit dem Divisor und subtrahieren das Resultat vom Dividenden.
Wir erhalten dann 66990. Die letzte von 0 verschiedene Ziffer des Resultates, d.h. 9, dividieren wir durch 7 und erhalten modulo 10

$$9 : 7 = 9 \cdot 3 = 7$$

Also ist die zweite Ziffer des Quotienten von rechts gleich 7. Nun multiplizieren wir wieder 7 mit dem Divisor und subtrahieren das Resultat von 66990. Wir erhalten 0, folglich ist die Division beendet und der Quotient gleich 78. Das Schema hat folgende Gestalt:

74646	|957^3
- 7656	| 78
6699	
-6699	
0	

Oben neben dem Divisor steht die Zahl, die in der Arithmetik modulo 10 der letzten Ziffer des Divisors reziprok ist. Die Division durch die letzte Ziffer des Divisors wird durch die Multiplikation mit dem Reziproken dieser Zahl ersetzt. Wir führen noch zwei Beispiele an:

61730684	|7459^3
- 44754	|8276
6168593	
- 52213	
611638	
- 14918	
59672	
-59672	
60	

217	| 3^7
- 27	|739
19	
- 9	
1	
- 21	
-2	

Beim zweiten Beispiel kommen wir zu einem negativen Rest. Das zeigt, dass die Division nicht mit ganzen Zahlen ausführbar ist. In Abschnitt 2.2. werden wir auf dieses Beispiel noch einmal zurückkommen.
Die von uns benutzte Divisionsmethode ist nicht unmittelbar anzuwenden, wenn der Divisor auf eine gerade Zahl oder auf 5 endet. In solchen Fällen werden der Dividend und der Divisor vorher durch 2 bzw. 5 gekürzt.[17]

Falls notwendig, wird das Kürzen mehrmals wiederholt, bis man schließlich einen Divisor erhält, der auf eine der Ziffern 1, 3, 7 und 9 endet. Danach wird die Division wie oben beschrieben ausgeführt.

Die beschriebene Methode ist in einer Reihe von Fällen einfacher und bequemer als die gewöhnliche. Die gewöhnliche Methode hat jedoch ihr gegenüber einen äußerst wichtigen Vorteil:
Falls die Division mit ganzen Zahlen nicht durchführbar ist, so gibt die allgemein übliche Methode die Möglichkeit, den Quotienten mit beliebiger, vorher festgelegter Genauigkeit zu finden; beispielsweise mit der Genauigkeit von 0,1 oder 0,001. Die oben beschriebene Methode gewährt jedoch diese Möglichkeit nicht.

38. Folgende Divisionen sind mit Hilfe der Arithmetik modulo 10 auszuführen:
a) 37233 : 189, b) 36408 : 328, c) 851 : 74.

2.2 Unendlich vielstellige Zahlen

In der Grundschule lernt man nur in solchen Fällen zu subtrahieren, in denen der Subtrahend kleiner als der Minuend ist. Versuchen wir, die gleichen Regeln für die Subtraktion einer Zahl von einer kleineren zu benutzen. Es soll beispielsweise die Differenz 398 - 536 berechnet werden.
Wir finden

$$\begin{array}{r} 0398 \\ -\ 536 \\ \hline \bar{1}862 \end{array}$$

Das Rechnen beginnt wie gewöhnlich mit den letzten Ziffern. Das einzig Neue ist, dass wir uns erlauben, von der 0 zu "borgen" und deshalb als erste Ziffer unseres Resultates die Zahl -1 erhalten. (Wir schreiben $\bar{1}$ statt -1, indem wir das Zeichen "-" über die Ziffer 1 schreiben, um deutlich zu machen, dass dieses Zeichen nur zu der ersten Ziffer gehört und nicht zu der gesamten Zahl.)
Das Resultat kann auch in folgender Form dargestellt werden: $(-1)\cdot 10^3+8\cdot 10^2+6\cdot 10+2$ oder $-1000+862$.

$$\begin{array}{r} \dot{0}\dot{0}\dot{1}0\dot{9}01 \\ -134521 \\ \hline \bar{1}876380 \end{array} \qquad \begin{array}{r} \dot{0}\dot{0}\dot{0}\dot{0}\dot{0}1 \\ -10002 \\ \hline \bar{1}89999 \end{array} \qquad \begin{array}{r} \dot{0}1889 \\ -2354 \\ \hline \bar{1}9535 \end{array}$$

[17] Die Division durch 5 kann durch die Multiplikation mit 2 und darauffolgende Division durch 10 ersetzt werden. Ebenso kann man, um durch 2 zu dividieren, erst mit 5 multiplizieren und anschließend durch 10 dividieren. Ist der Dividend nicht in ganzen Zahlen durch 2 oder 5 zu dividieren, so erhalten wir nach dem Kürzen einen Dezimalbruch.

Kehren wir nun zu dem schon betrachteten Beispiel 217 : 3 zurück. Wir hatten dessen Betrachtung abgebrochen, als wir zu einem negativen Rest kamen und feststellten, dass die Division in ganzen Zahlen unmöglich ist. Nunmehr setzen wir die abgebrochene Rechnung fort, wobei wir die Division so ausführen werden, wie es eben beschrieben wurde.

$$\begin{array}{rl} 217 & |3^7 \\ -27 & |...66739 \\ \hline 19 & \\ 9 & \\ \hline \dot{0}01 & \\ 21 & \\ \hline \dot{0}\overline{1}8 & \\ 18 & \\ \hline \dot{0}\overline{1}8 & \\ 18 & \\ \hline \overline{1}8 & \end{array}$$

Bei Fortsetzung der Division erhalten wir stets nur den Rest ($\overline{1}8$) und gleichzeitig immer wieder die gleiche Ziffer (6) für den Quotienten. Daher ist das Resultat dieser Division eine ganze periodische Zahl mit unendlich vielen Stellen, nämlich ...6666739.
Wir kontrollieren, ob diese Zahl bei der Multiplikation mit 3 die Zahl 217 ergibt.
In der Tat ist

$$\begin{array}{r} ...6666739 \\ \cdot \quad 3 \\ \hline ...0000217 \end{array}$$

Alle Ziffern des Produktes außer den letzten drei sind also Nullen.
Somit kann also die neue Divisionsmethode ebenso wie die allgemein übliche Methode zu einer Lösung führen, die sich als unendliche Folge von Ziffern schreiben lässt; nur ist diese Folge nicht nach rechts, sondern nach links unendlich: Statt eines unendlichen Dezimalbruches erhalten wir eine ganze Zahl mit unendlich vielen Stellen.

Bei Zahlen mit unendlich vielen Stellen kann man die Addition, Subtraktion und Multiplikation nach denselben Regeln ausführen wie bei mehrstelligen Zahlen. Dabei genügt es zur Berechnung der letzten n Ziffern des Resultate, die letzten n Ziffern jeder der Zahlen zu kennen, die man addieren, subtrahieren oder multiplizieren soll. Wir nehmen als Beispiele:

$$\begin{array}{r} ...100010010 \\ +...000990090 \\ \hline ... \ 101000100 \end{array} \qquad \begin{array}{r} ...175321 \\ \cdot \ ...531498 \\ \hline ...402568 \\ ...577889 \\ +...701284 \\ ...175321 \\ ...525963 \\ ...876605 \\ \hline ...760858 \end{array}$$

Wir betrachten nun die Division. Wenn der Dividend auf eine der Ziffern 1, 3, 7, 9 endet, kann die Division nach der in 2.1. beschriebenen Methode ausgeführt werden. Beispielsweise

$$\begin{array}{l|l} \ldots23517 & \ldots85143^{7} \\ \ldots66287 & \ldots40619 \\ \hline \ldots5723 & \\ \ldots5143 & \\ \hline \ldots058 & \\ \ldots858 & \\ \hline \ldots20 & \\ 2 & \end{array}$$

Das Resultat der Division ist wieder eine ganze Zahl mit unendlich vielen Stellen.
Komplizierter wird es, wenn der Divisor auf eine der Ziffern 0, 2, 4, 5, 6, 8 endet: In diesen Fällen gelingt es durchaus nicht immer, eine ganze Zahl mit unendlich vielen Stellen zu finden, die bei der Multiplikation mit dem Divisor den Dividenden ergibt.

Es möge beispielsweise der Dividend auf 1 enden und der Divisor 10 sein. Welche unendlich stellige ganze Zahl wir mit 10 multiplizieren, stets wird das Produkt eine Null als letzte Ziffer haben; es kann folglich niemals gleich dem Dividenden sein.
Demnach ist es unmöglich, eine Zahl, die mit 1 endet, im Gebiet der ganzen Zahlen mit unendlich vielen Stellen durch 10 zu dividieren. Ein natürlicher Ausweg besteht darin, gebrochene Zahlen mit unendlich vielen Stellen zu betrachten, wie beispielsweise ... 66739,1 oder ... 56429,0000017 usw., d.h. Zahlen, die endlich viele Stellen hinter dem Komma haben.

Die Addition, Subtraktion und Multiplikation dieser Zahlen werden nach den gleichen Regeln ausgeführt wie bei der Rechnung mit gewöhnlichen Dezimalbrüchen; zusätzliche Erklärungen sind nicht notwendig.

Nach der Einführung der gebrochenen Zahlen mit unendlich vielen Stellen wird die Division durch 10 leicht ausführbar. Sie lässt sich auf die Verschiebung des Kommas um eine Stelle nach links zurückführen. Gleichzeitig wird auch die Division durch 2 und 5 leicht ausführbar: Sie wird auf die Division durch 10 und die Multiplikation mit 5 bzw. 2 zurückgeführt.

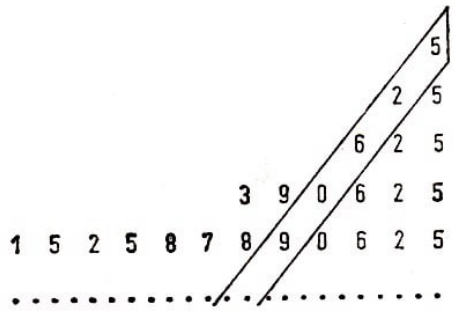
Wenn wir durch 2, 5 und jede beliebige Zahl, die mit 1, 3, 7 oder 9 endet, dividieren können, so haben wir damit die Möglichkeit, durch jedes beliebige Produkt der Form $2^m 5^n a$ zu dividieren:
Um durch $2^m 5^n a$ zu dividieren, genügt es, m-mal durch 2, n-mal durch 5 und dann durch a zu dividieren.
Da jede beliebige Zahl mit endlich vielen Stellen in der angegebenen Form ausgedrückt werden kann, ist somit die Division durch Zahlen mit endlich vielen Stellen stets ausführbar. Ist der Divisor jedoch eine Zahl mit unendlich vielen Stellen, so kann man nicht erwarten, dass man ihn in der Form $2^m 5^n a$, wobei a auf eine der Ziffern 1, 3, 7 oder 9 endet, darstellen kann. Tatsächlich zeigen Beispiele (siehe Aufgabe 41), dass die Division durch Zahlen mit unendlich vielen Stellen nicht immer ausführbar ist, selbst

wenn gebrochene Zahlen mit unendlich vielen Stellen benutzt werden.[18]

Abschließend weisen wir auf eine Ähnlichkeit zwischen der Arithmetik der Zahlen mit unendlich vielen Stellen und der Arithmetik modulo 10 hin:
In jeder der beiden sind Addition, Subtraktion und Multiplikation stets ausführbar, wobei für diese Operationen alle Gesetze der gewöhnlichen Arithmetik gelten; in jeder dieser Arithmetiken ist jedoch die Division nicht immer ausführbar.

39. Es sind ganze periodische Zahlen mit unendlich vielen Stellen zu finden, die die Verhältnisse 1 : 3, 1 : 7 und 1 : 9 ausdrücken. Die Resultate sind durch Multiplikation zu verifizieren.

40. Man beweise, dass in der Tabelle



in der jede Zahl von der zweiten (von oben) ab durch Quadrieren der über ihr stehenden Zahl gewonnen wird,
a) die (eingerahmte) unendlich vielstellige Zahl $d = ...90625$ gleich ihrem Quadrat ist, also $d^2 = d$ gilt;
b) die Zahl $e = 1 - d = ...09376$ die gleiche Eigenschaft hat (also $e^2 = e$ ist);
c) $d \cdot e = 0$ ist.
Hinweis. Man zeige vorher, dass bei der n-ten und der $(n+1)$-ten Zahl der Tabelle die letzten n. Ziffern übereinstimmen.

41. Es ist zu beweisen, dass die Zahl d, die in der vorhergehenden Aufgabe konstruiert wurde, keine Reziproke hat, d.h., dass man keine (ganze oder gebrochene) Zahl x mit unendlich vielen Stellen finden kann derart, dass $x \cdot d = 1$ gilt.

42. Man beweise, dass der Bedingung $x^2 = x$ nur vier Zahlen mit unendlich vielen Stellen genügen; die Zahl 0, die Zahl 1 sowie die in Aufgabe 40 konstruierten Zahlen $d = ...90625$ und $e = ...09376$.

[18] Der Leser könnte fragen, warum man nicht Zahlen mit unendlich vielen Stellen hinter dem Komma betrachtet, d.h. Zahlen, die in beiden Richtungen unendlich sind. Dies beruht darauf, dass für solche Zahlen unmöglich die Rechengesetze (Addition usw.) sinnvoll definiert werden können; bildlich ausgedrückt, man kann diese Zahlen "von nirgends her anpacken".

2.3 m-adische und p-adische Zahlen

2.3.1 Positionssysteme

In den vorhergehenden Abschnitten spielte die Zahl 10 eine besondere Rolle. Der Grund dafür ist der, dass 10 die Basis des meistbenutzten m-adischen Systems ist:
Wenn eine mehrstellige Zahl mit Hilfe der Ziffern $a_n, a_{n-1}, ..., a_1, a_0$ geschrieben wird, so ist sie gleich

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

Die hervorragende Rolle der 10 wird selbstverständlich nicht durch irgendwelche mathematischen Vorzüge dieser Zahl im Vergleich zu anderen natürlichen Zahlen bestimmt, sondern liegt in der Entstehungsgeschichte des Zählens begründet, die untrennbar mit dem Abzählen an den Fingern verbunden ist.

Statt der 10 kann als Basis eines Positionssystems jede beliebige andere Zahl $m \neq 1$ genommen werden; unter allen diesen m-adischen Systemen ist das dekadische nur dadurch ausgezeichnet, dass wir daran gewöhnt sind.

Wir betrachten ein vom dekadischen (Dezimalsystem) verschiedenes m- adisches System näher, beispielsweise das 5-adische. Hier existieren nur die fünf verschiedenen Ziffern 0, 1, 2, 3, 4; der Ausdruck 122 bedeutet im 5-adischen System $1 \cdot 5^2 + 2 \cdot 5 + 2$, d.h. siebenunddreißig; der Ausdruck 2001 bedeutet die Zahl $2 \cdot 5^3 + 0 \cdot 5^2 + 0 \cdot 5 + 1$, also zweihunderteinundfünfzig.

Allgemein ist eine Zahl, die im m-adischen System durch die Ziffern $a_n, a_{n-1}, ..., a_1, a_0$ beschrieben wird, gleich

$$a_n \cdot m^n + a_{n-1} \cdot m^{n-1} + ... + a_1 \cdot m + a_0$$

Wir zeigen nun, wie man vom dekadischen System zum 5-adischen übergeht. Als Beispiel betrachten wir die Zahl 1666 (sechzehnhundertsechsundsechzig) und schreiben

$$\begin{aligned} 1666 &= 5 \cdot 333 + 1, \\ 333 &= 5 \cdot 66 + 3, \\ 66 &= 5 \cdot 13 + 1, \\ 13 &= 5 \cdot 2 + 3, \\ 2 &= 5 \cdot 0 + 2. \end{aligned}$$

Die erste dieser Gleichungen drückt aus, dass die Zahl 1666 bei Division durch 5 den Quotienten 333 und den Rest 1 ergibt. Analog drücken die übrigen Gleichungen das Ergebnis der Division der aufeinanderfolgenden Quotienten 333, 66, 13 und 2 durch 5 aus.
Im 5-adischen System nimmt die Zahl 1666 demnach die Form 23131 an; ihre Ziffern sind die von uns gefundenen Reste.

Die Addition, Subtraktion und Multiplikation mehrstelliger Zahlen werden im 5-adischen System nach den gleichen Regeln ausgeführt wie im dekadischen. Dabei ist es vorteilhaft, Additions- und Multiplikationstabellen im 5-adischen System zu benutzen.

Additionstafel

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

Multiplikationstafel

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

Zur Illustration der Rechenoperationen im 5-adischen System führen wir einige Beispiele an:

$$\begin{array}{r} 4302 \\ +3043 \\ \hline 12400 \end{array} \qquad \begin{array}{r} 13404 \\ -\ 441 \\ \hline 344 \end{array} \qquad \begin{array}{r} 421 \\ \cdot\ 432 \\ \hline 1342 \\ +2313 \\ 3234 \\ \hline 403422 \end{array}$$

Alles über das 5-adische System Gesagte gilt genau so für jedes andere m-adische System. Die einzige zusätzliche Bemerkung, die gemacht werden muss, betrifft die Kennzeichnung der Ziffern.
Ein m-adisches System hat m verschiedene Ziffern. Ist $m > 10$, so genügen die üblichen Zeichen 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 nicht zu ihrer Unterscheidung. Es ist notwendig, zusätzliche Zeichen einzuführen.
Beispielsweise braucht man im 12-adischen System neue Symbole zur Bezeichnung der Zahlen 10 und 11. Als solche Zeichen könnte man beispielsweise die Buchstaben α und β nehmen.

2.3.2 m-adische Zahlen

Wir gehen einen Schritt weiter und betrachten im m-adischen System nicht nur mehrstellige Zahlen, sondern Zahlen mit unendlich vielen Stellen, d.h. Folgen von Ziffern im m-adischen System, die von rechts nach links unendlich sind.

Da der Begriff "Zahlen mit unendlich vielen Stellen" nichts darüber aussagt, welches System zugrunde gelegt ist, verwendet man den genaueren Ausdruck "m-adische Zahlen".
Die Addition, Subtraktion und Multiplikation m-adischer Zahlen unterscheiden sich von den in Abschnitt 2.2. behandelten entsprechenden Rechenoperationen mit dekadischen Zahlen nicht mehr, als sich die Rechenoperationen mit mehrstelligen Zahlen in einem m-adischen System von denen im dekadischen System unterscheiden.

Zur Illustration führen wir einige Beispiele der Addition, Subtraktion und Multiplikation 5-adischer Zahlen an:

		...43001
		·...32104
...3333,1034	...13203,1	...32004
+...1111,432	-...21403,2	...001
...0000,0404	...41244,4	...02
		...3
		...14104

Bereits in Abschnitt 2.2. wiesen wir die Ähnlichkeit zwischen der Arithmetik der dekadischen Zahlen und der Arithmetik modulo 10 hin. Wir können nunmehr sagen, dass die Arithmetik der m-adischen Zahlen und die Arithmetik modulo m im gleichen Verhältnis stehen.

2.3.3 p-adische Zahlen

In der Restklassenarithmetik nehmen die Restklassen modulo einer Primzahl eine besondere Stellung ein. Es sind daher gerade von den p- adischen Zahlen besonders interessante Eigenschaften zu erwarten. Und in der Tat, diese Eigenschaften zeigen sich, sobald wir uns der Division zuwenden:

Im Bereich der p-adischen Zahlen ist die Division stets ausführbar. Wir wollen nun beschreiben, wie sie auszuführen ist. Ist die letzte Ziffer des Divisors ungleich Null, so lässt sich eine Zahl finden, die dieser letzten Ziffer im Sinne der Restklassenarithmetik reziprok ist (eine solche existiert immer).
Diese reziproke Zahl schreiben wir oben neben den Divisor und führen die Division ganz analog der in Abschnitt 2.2. behandelten Division durch einen auf 1, 3, 7 oder 9 endenden Divisor aus.
Wir führen einige Beispiele für 7-adische Zahlen an.

		Probe
$...\dot{0}01$	$\mid 3^5$	
- 21	$\mid ...445$	...445
$0\overline{1}5$		· 3
- 15		...001
$\overline{1}5$		

		Probe
...163	$\mid ...346^6$	...346
-...053	$\mid ...064$	·...064
...11		...053
-...111		+...11
...		...0
		...163

Wenn der Divisor auf k Nullen endet, so ist seine Form $p^k \cdot a$, wobei die letzte Ziffer der Zahl a ungleich Null ist. Die Division durch eine solche Zahl lässt sich auf die Division

durch p^k zurückführen, indem man das Komma um k Stellen nach links rückt und anschließend auf bekannte Art durch a dividiert.

Beispielsweise wird die Division der 7-adischen Zahl ..163 durch die 7-adische Zahl ...34600 folgendermaßen ausgeführt:

$$...163 : ...34600 = (...163 : 100)1...346 = ...1,63 : ...346 = ...0,64$$

Folglich bilden die (ganzen und die gebrochenen) p-adischen Zahlen ein System, in dem genau wie in der Restklassenarithmetik modulo p die vier Rechenoperationen Addition, Subtraktion, Multiplikation und. Division stets ausführbar sind.

2.3.4 Geometrische Progressionen

Eine Folge p-adischer Zahlen

$$b_0, b_1, b_2, ..., b_n, ...$$

heißt geometrische Progression (auch Folge), wenn jedes der Glieder, angefangen bei b_1, aus dem vorhergehenden durch Multiplikation mit einer konstanten Zahl q, dem Quotienten der Folge, entsteht, d.h. $b_n = b_{n-1} \cdot q$ $(n \geq 1)$. Wir setzen dabei stets $b \neq 0$ und $q \neq 0$ voraus (andernfalls artet die Progression in eine Nullfolge aus).
In den Aufgaben 43 bis 45 werden geometrische Progressionen betrachtet, deren Glieder ganze p-adische Zahlen sind.

43. Es sei a eine beliebige ganze p-adische Zahl, deren letzte Ziffer ungleich Null ist. Es ist zu beweisen, dass die letzte Ziffer der Zahl $a^{p-1} - 1$ gleich 0 ist. (Falls er eine Zahl mit endlich vielen Stellen ist, stimmt diese Aufgabe mit Aufgabe 16 überein.)

44. Es sei a eine ganze p-adische Zahl, deren letzte Ziffer ungleich 0 ist. Man beweise, dass die Zahl $a^{p^{k+1}(p-1)} - 1$ auf k Nullen endet.

45. Werden bei allen Gliedern der geometrischen Progression $b_0, b_1, ..., b_n, ...$ (alle b_i sind ganze p-adische Zahlen; der Quotient der Folge ist nicht durch p teilbar) nur die letzten k Ziffern beibehalten, so entsteht eine periodische Folge, deren Länge ein Teiler der Zahl $p^{k-1}(p-1)$ ist. Mit anderen Worten: Man beweise, dass b_n und $b_{n+p^{k+1}(p+1)}$ auf dieselben k Ziffern enden.

2.3.5 Quadratwurzelziehen. Quadratische Gleichungen

46. Man beweise, dass die Gleichung $x^2 = a.$ in der Arithmetik p-adischer Zahlen entweder zwei oder gar keine Lösungen hat.

47. Man leite die Formel zur Lösung der quadratischen Gleichung

$$ax^2 + bx + c = 0$$

(a, b und c sind p-adische Zahlen, $a \neq 0$) her.

Wir versuchen nun, eine Methode zum Wurzelziehen aus p-adischen Zahlen zu finden. Dabei genügt es, das Wurzelziehen aus ganzen Zahlen zu betrachten.

Hat die Zahl k Ziffern nach dem Komma, so gehen wir folgendermaßen vor:

Wir multiplizieren sie mit p^{2k} (die Zahl wird dann eine ganze Zahl), danach ziehen wir die Wurzel und dividieren schließlich das Resultat durch p^k.

48. Man beweise, dass die Quadratwurzel aus einer ganzen p-adischen Zahl eine ganze Zahl ist.

49. Lässt sich aus einer bestimmten p-adischen Zahl die Quadratwurzel ziehen, so kann in der Arithmetik modulo p die Quadratwurzel aus der letzten Ziffer dieser Zahl gezogen werden.

Endet eine ganze p-adische Zahl auf eine ungerade Anzahl von Nullen, so ist es, unmöglich, aus ihr die Quadratwurzel zu ziehen; denn endet eine bestimmte Zahl auf k Nullen, so endet ihr Quadrat auf $2k$ Nullen. Endet eine Zahl auf $2k$ Nullen, so kann man alle diese Nullen fortlassen (mit anderen Worten, durch p^{2k} dividieren), aus der erhaltenen Zahl die Quadratwurzel ziehen und zu dem Resultat k Nullen hinzufügen (mit p^k multiplizieren).
Daher lässt sich das Quadratwurzelziehen aus beliebigen p-adischen Zahlen auf das Quadratwurzelziehen aus ganzen p-adischen Zahlen, deren letzte Ziffer keine Null ist, zurückführen.

Wir zeigen jetzt, wie die Quadratwurzel aus einer p-adischen Zahl gezogen wird, wenn die letzte Ziffer dieser Zahl von Null verschieden ist und man aus dieser Zahl im Sinne der Arithmetik modulo p die Quadratwurzel ziehen kann (der Fall $p = 2$ wird ausgeschlossen).
Wir lernen zuerst, die Quadratwurzel mit einer Genauigkeit von n Ziffern zu ziehen. Wir nennen die p-adische Zahl B_n eine Quadratwurzel mit der Genauigkeit von n Ziffern aus der p-adischen Zahl A, wenn B_n^2 und A die letzten n Ziffern gemeinsam haben.

50. Man weise nach, dass in der triadischen Arithmetik die Zahl 201 eine Quadratwurzel mit der Genauigkeit von drei Ziffern aus der Zahl ...112101 ist.[19]

Angenommen, wir hätten $B - n$ bereits gefunden. Wir zeigen jetzt, wie in diesem Falle B_{n+1} als die Quadratwurzel aus A mit der Genauigkeit von $n+1$ Ziffern gefunden wird. Wir suchen B_{n+1} in der Form [20]

$$B_{n+1} = B_n + x \cdot 10^n$$

wobei x eine einstellige p-adische Zahl ist ($x \cdot 10^n = x\underbrace{00..00}_{n \text{ Nullen}}$). Erheben wir B_{n+1} ins Quadrat, so erhalten wir

$$B_{n+1}^2 = B_n^2 + 2B_n \cdot x \cdot 10^n + x^2 \cdot 10^{2n}$$

woraus

$$2B_n \cdot x \cdot 10^n = B_{n+1}^2 - B_n^2 - x^2 \cdot 10^{2n} \quad (1)$$

[19] Wir verwenden die Schreibweise 201 statt ...000201. Jede Zahl mit endlich vielen Stellen im m-adischen System kann auf diese Art als m-adische Zahl betrachtet werden.

[20] Wir weisen darauf hin, dass die Zahl p in der p-adischen Arithmetik als 10 geschrieben wird.

folgt. Wir müssen erreichen, dass die letzten $n+1$ Ziffern von B_{n+1}^2 mit denen von A übereinstimmen.
Aus der Formel (1) folgt, dass dafür notwendig und hinreichend ist, dass die Zahlen $2 \cdot B_n \cdot x \cdot 10^n$ und $A - B_n^2 - x^2 \cdot 10^{2n}$ dieselben letzten $n+1$ Ziffern haben oder, was das gleiche ist, dass dies für die Zahlen $2 \cdot B_n \cdot x \cdot 10^n$ und $A - B_n^2$ gilt (da $x^2 \cdot 10^{2n}$ auf $2n$ Nullen endet).

Somit müssen die letzten $n+1$ Ziffern der Zahlen $2B_n \cdot x \cdot 10^n$ und $A - B_n^2$ übereinstimmen.
Sowohl $2B_n \cdot x \cdot 10^n$ als auch $A - B_n^2$ enden auf n Nullen, so dass die letzten n Ziffern automatisch übereinstimmen. Die letzte Ziffer der Zahl B_n sei b (da nach Voraussetzung die letzte Ziffer von A ungleich Null sein sollte, folgt $b = 0$).
Danach ist die letzte Ziffer der Zahl $2B_n$ gleich $c = 2b$ (das Produkt von 2 und b in der Arithmetik modulo p) mit $c \neq 0$, da $p \neq 2$ und $b \neq 0$ ist.

In diesem Fall ist c von rechts aus die $(n+1)$-te Ziffer der Zahl $2B_n \cdot 10^n$; die $(n+1)$-te Ziffer von $2B_n \cdot 10^n \cdot x$ ist cx (das Produkt von c und x in der Arithmetik modulo p). Wenn wir die $(n+1)$-te Ziffer der Zahl $A - B_n^2$ mit d bezeichnen, so erhalten wir

$$cx = d$$

hieraus folgt, dass $x = \frac{d}{c}$ in der Restklassenarithmetik modulo p ist (wegen $c \neq 0$ ist die Division ausführbar). Wir haben damit B_{n+1} gefunden. Wir weisen noch darauf hin, dass bei B_{n+1} und B_n die letzten n Ziffern übereinstimmen.

Beispiel. Man bestimme die Quadratwurzel aus der triadischen Zahl ...112101 mit einer Genauigkeit von vier Ziffern. Die Quadratwurzel bis zur Genauigkeit von drei Stellen kennen wir bereits (siehe Aufgabe 50); sie ist 201. Die gesuchte Zahl muss die Form $(201 + x \cdot 10^3)$ haben. Es ist

$$(201 + x \cdot 10^3)^2 = 201^2 2 \cdot 201 \cdot x \cdot 10^3 + x^2 \cdot 10^6 = 111101 + 1102000 \cdot x + x^2 \cdot 10^6$$

Die letzten vier Ziffern dieser Zahl stimmen mit den entsprechenden Ziffern der Zahl ...112101 überein. Das ist gleichbedeutend damit, dass die letzten vier Ziffern der Zahl $1102000 \cdot x$ den letzten vier Ziffern der Zahl

$$...112101 - 111101 - x^2 \cdot 10^6 = ...001000 \tag{2}$$

gleich sind; die Zahl $1102000 \cdot x$ hat (in der Restklassenarithmetik modulo 3) $2x$ als vierte Ziffer von rechts, bei der Zahl (2) ist diese Ziffer 1. Daraus folgt modulo 3

$$2x = 1$$

und $x = 2$. Wir überlassen es dem Leser, nachzuprüfen, dass $201 + 2 \cdot 10^3 = 2201$ tatsächlich die Quadratwurzel aus 112101 mit der Genauigkeit von vier Ziffern ist.

Wir sind nunmehr in der Lage, die Quadratwurzel aus einer p-adischen Zahl A zu ziehen. Die letzte Ziffer von A sei a_1.

Ist $\sqrt{a_1}$ in der Arithmetik modulo p zu bestimmen, so ist $a_1 = b_1^2$. Dann ist die p-adische Zahl $B_1 = ...00b_1$ Quadratwurzel aus A mit einer Genauigkeit von einer Ziffer.
Durch Anwendung unseres Verfahrens berechnen wir sukzessive B_2, B_3, ..., B_n, ...
Wir schreiben diese Zahlen untereinander auf :

$$\begin{aligned} .....b_1 &= B_1 \\ .....b_2b_1 &= B_2 \\ .....b_3b_2b_1 &= B_3 \\ ...b_4b_3b_2b_1 &= B_4 \end{aligned}$$

Die Ziffern, die auf der Hauptdiagonale dieser Tabelle stehen, bilden die p-adische Zahl $B = ...b_4b_3b_2b_1$. Es ist leicht einzusehen, dass $B_2 = A$ ist.
Wenn wir hierbei die Aufgabe 49 anwenden, erhalten wir daraus folgendes Resultat:

Es sei $p \neq 2$ und die letzte Ziffer einer p-adischen Zahl A ungleich Null; man kann die Quadratwurzel aus A dann und nur dann ziehen, wenn sich aus der letzten Ziffer von A die Quadratwurzel in der Arithmetik modulo p ziehen lässt.

3 Anwendungen der Arithmetik der Restklassen modulo m und modulo p in der Zahlentheorie

3.1 Die Fibonaccische Folge

Eine Zahlenfolge

$$u_0, u_1, u_2, ..., u_n, ...$$

heißt Fibonaccische Folge (abgekürzt F-Folge), wenn jedes ihrer Glieder, angefangen bei u_2 gleich der Summe der beiden vorhergehenden ist, d.h.

$$u_n = u_{n-2} + u_{n-1} \qquad (\text{für } n \geq 2)$$

Folglich ist eine F-Folge vollständig bestimmt, wenn man ihre beiden Anfangsglieder u_0 und u_1 angibt.

Durch verschiedene Wahl der Zahlen u_0 und u_1 erhalten wir verschiedene Fibonaccische Folgen. Eine besondere Rolle unter diesen Folgen spielt diejenige, die mit den Zahlen 0 und 1 beginnt, d.h. die Folge

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ...$$

Wir wollen verabreden, diese Folge mit F^0 und ihre Glieder mit den Buchstaben $a_0, a_1, a_2, ...$ zu bezeichnen:

$$a_0 = 0, a_1 = 1, a_2 = 1, a_3 = 2, a_4 = 3, a_5 = 5, a_6 = 8, ...$$

3.1.1 Einige Beziehungen zwischen den Zahlen der Fibonaccischen Folge

51. Es sei $u_0, u_1, u_2, ..., u_n, ...$ eine beliebige Fibonaccische Folge. Man beweise, dass sich das n-te Glied dieser Folge durch u_0 und u_1 gemäß der Formel

$$u_n = a_{n-1}u_0 + a_n u_1$$

ausdrücken lässt. (Man muss $a_{-1} = 1$ annehmen, damit die Formel für $n = 0$ ihre Gültigkeit behält.)

52. Man beweise die Formel

$$a_{n+m-1} = a_{n-1}a_{m-1} + a_n a_m$$

53. Man beweise, dass die Summe der Quadrate zweier benachbarter Zahlen der Folge F^0 (d.h. $a_{n-1}^2 + a_n^2$) wieder der Folge F^0 angehört.

54. Wählt man aus der Folge F^0 drei beliebige aufeinanderfolgende Glieder a_{n-1}, a_n, a_{n+1} aus, multipliziert die äußeren Glieder miteinander und subtrahiert von diesem Produkt das Quadrat des mittleren Gliedes, so erhält man 1 oder -1.
Man beweise, dass für eine beliebige Fibonaccische Folge (die nicht unbedingt mit den Zahlen 0 und 1 beginnen muss) der Ausdruck $u_{n-1} \cdot u_{n+1} - u_n^2$ für jedes n den gleichen absoluten Betrag hat.

55. Werden aus der Folge F^0 vier aufeinanderfolgende Glieder $a_{n-1}, a_n, a_{n+1}, a_{n+2}$ ausgewählt und wird von dem Produkt der äußeren Glieder a_{n-1}, a_{n+2} das Produkt der inneren Glieder a_n, a_{n+1} subtrahiert, so erhält man 1 oder -1.
Man beweise, dass im Falle einer beliebigen Fibonaccischen Folge der absolute Betrag des Ausdruckes $u_{n-1} \cdot u_{n+2} - u_n \cdot u_{n+1}$ von n unabhängig ist.

3.1.2 Fibonaccische Folgen in einer Arithmetik modulo m

Eine Folge

$$v_0, v_1, v_2, ..., v_n, ...$$

von Elementen aus einer Arithmetik modulo m heißt Fibonaccische Folge in der Arithmetik modulo m (abgekürzt F_m-Folge), wenn für $n \geq 2$

$$v_n = v_{n-2} + v_{n-1} \qquad (\text{modulo } m)$$

gilt (die Addition ist im Sinne der Arithmetik modulo m zu verstehen).
Wie in der gewöhnlichen Arithmetik wird die Folge F_m durch ihre beiden Anfangsglieder v_0 und v_1 bestimmt. Beispielsweise lautet die Folge F_{11}, die mit den Zahlen 4 und 5 beginnt,

$$4, 5, 9, 3, 1, 4, 5, ...$$

Besondere Bedeutung hat die Folge, die mit den Elementen 0 und 1 beginnt. Wir wollen sie mit F_m^0 und ihre Glieder durch die Buchstaben c_0, c_1, c_2, ..., c_n, ... bezeichnen. Beispielsweise lautet die Folge F_5^0:

$$0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, ...$$

Die Formeln, die in den Aufgaben 51-55 abgeleitet wurden, sind auch für Folgen in einer Arithmetik modulo m gültig, wenn in ihnen u_0, u_1, u_2, ... und a_0, a_1, a_2, ... durch v_0, v_1, v_2, ... ersetzt werden.
Setzt man unter jede Zahl der Folge F^0

$$0, 1, l, 2, 3, 5, 8, 13, 21, 34, ...$$

den Rest der Zahl bei Division durch m, so bilden die Reste die Folge F_m^0.

3.1.3 Die Verteilung der durch m teilbaren Zahlen in einer Fibonaccischen Folge

56. Man zeige, dass die letzten Ziffern der Zahlen der Folge F^0 periodisch wiederkehren. Wie groß ist die Länge der Periode?

57. (Verallgemeinerung der Aufgabe 56). Man beweise, dass alle F_m-Folgen periodisch sind, wobei die Länge der Periode jeweils höchstens m^2 ist.

58. Es sei m eine beliebige ganze Zahl. Man beweise, dass in der Folge F^0

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ...$$

unendlich viele durch m teilbare Zahlen vorhanden sind.[21]

Ein System von n Elementen aus einer Arithmetik modulo m, die auf einem Kreis in gleichen Abständen angeordnet sind, nennt man Fibonaccische Kreisfolge modulo m, abgekürzt $\widehat{F}_m$ (lies "F_m Bogen"), wenn bei Bewegung im Uhrzeigersinne jedes Glied der Folge gleich der Summe der beiden vorhergehenden ist. In Abb. B.4 sind Beispiele aus der $\widehat{F}_5$-Folge angeführt.

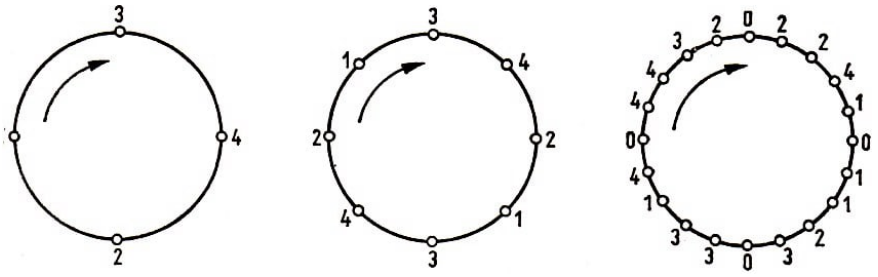


Abb. B.4

Wir wollen eine Folge $\widehat{F}_m$ als Folge ohne Wiederholungen bezeichnen, wenn sie bei keiner Drehung um einen Winkel, der größer als 0° und kleiner als 360° ist, mit sich selbst zur Deckung gebracht werden kann.
Bei den in Abb. 3.4 angeführten Folgen sind die erste und dritte Folge Folgen ohne Wiederholungen. Die zweite Folge ist eine Folge mit Wiederholungen, da sie bei einer Drehung um 180° mit sich selbst zur Deckung kommt.

Tritt in einem F_m zweimal das gleiche Paar benachbarter Elemente auf, so ist F_m eine Folge mit Wiederholungen. Denn hat eine Folge die in Abb. B.5 dargestellte Form und ist $x = u, y = v$, so kommt sie bei einer Drehung, die x in u und y in v überführt, mit sich zur Deckung.

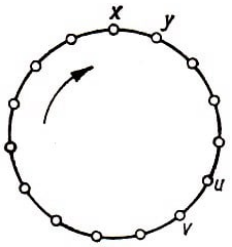


Abb. B.5

Entsprechend der Aufgabe 57 ist jede Folge F_m periodisch. Deshalb genügt es zur Untersuchung solcher Folgen, nur die Glieder, die die erste Periode darstellen, zu beachten. Werden diese Zahlen auf einem Kreis im Uhrzeigersinn aufgeschrieben, so erhält man eine F_m-Folge ohne Wiederholungen.

59. Man stelle die Folgen

$$\widehat{F}_2^0, \widehat{F}_3^0, \widehat{F}_4^0, ..., \widehat{F}_{10}^0, \widehat{F}_{11}^0$$

[21] In der zweiten Runde der IX. Moskauer Mathematischen Olympiade für 9. und 10. Klassen wurde folgender Spezialfall dieser Aufgabe vorgelegt: Man beweise, dass unter den ersten 10^8+1 Gliedern der Fibonaccischen Folge

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ...$$

Zahlen vorkommen, die auf vier Nullen enden.

auf (durch das Zeichen $\widehat{F}_m^0$, wird eine Folge F_m ohne Wiederholung bezeichnet, die das Paar 0, 1 enthält).

60. Es seien x und y zwei Elemente der Folge $\widehat{F}_m^0$. Ist in der Folge $\widehat{F}_m^0$ eine Null enthalten, die von x und y gleichen Abstand hat[22] (siehe Abb. B.6), so ist entweder $x + y = 0$ oder $x - y = 0$.

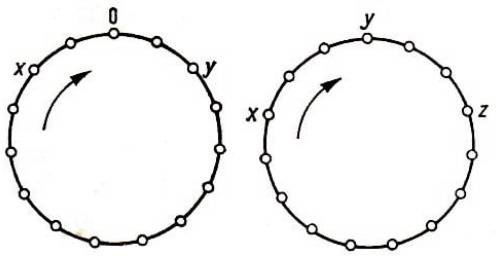


Abb. B.6 und B.7

61. Die drei Elemente x, y, z der Folge $\widehat{F}_m$ seien so angeordnet, dass die Entfernung zwischen x und y gleich der Entfernung zwischen y und z ist (siehe Abb. 3.7). Man beweise: Aus $x = y = 0$ folgt $z = 0$.

62. Man beweise, dass die Nullen, die in der Folge $\widehat{F}_m$ enthalten sind, diese Folge in gleichlange Abschnitte aufspalten.

63. Man beweise, dass in der Folge F^0

$$0, 1, 1, 2, 3, 5, 8, 13, ...$$

die durch m teilbaren Zahlen in gleichen Abständen voneinander liegen.

64. Enthält die Kreisfolge ohne Wiederholungen, $\widehat{F}_m$ Nullen und besteht sie aus einer ungeraden Anzahl von Elementen, so ist die Anzahl dieser Elemente gleich 3.

65. Man beweise, dass die Anzahl der Nullen, die in einer Kreisfolge $\widehat{F}_m$ ohne Wiederholungen enthalten sind, gleich 0, 1, 2 oder 4 ist. (Daraus folgt, dass in einer Periode einer F_m-Folge die Anzahl der Nullen gleich 0, 1, 2 oder 4 ist.)

3.1.4 Die Fibonaccische und die geometrische Folge

Eine Folge von Elementen

$$b_0, b_1, b_2, ..., b_n, ...$$

aus einer Arithmetik modulo m heißt geometrische Progression (Folge), wenn jedes ihrer Glieder, angefangen bei b_1 durch Multiplikation mit einer konstanten Zahl q, dem Quotienten der Folge, aus dem vorhergehenden Glied entsteht. Beispielsweise haben wir in der Arithmetik modulo 7 für $b_0 = 5$, $q = 3$ die geometrische Progression

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

in der Arithmetik modulo 12 für $b_0 = 1$, $q = 2$ die geometrische Folge

$$1, 2, 4, 8, 4, 8, 4, ...$$

[22] In dem Sinne, dass die Bögen $\widehat{x0}$ und $\widehat{y0}$ die gleiche Anzahl Glieder der Folge enthalten.

Das allgemeine Glied b_n einer geometrischen Folge lässt sich durch das Anfangsglied b_0 und den Quotienten q durch $b_n = b_0 q^n$ ausdrücken, was man wie in der Schulmathematik beweisen kann.
Wir werden hier nur solche geometrischen Folgen betrachten, bei denen $b_0 \neq 0$ und $q \neq 0$ ist (sonst artet die Folge in eine Nullfolge aus).

66. Die periodische Folge

$$1, 4, 5, 9, 3, 1, 4, 5, 9, 3, 1, 4, 5, 9, 3, ... \tag{1}$$

von Elementen der Arithmetik modulo 11 ist gleichzeitig geometrische Folge und Fibonaccische Folge. Die gleiche Eigenschaft hat die Folge

$$b, 4b, 5b, 9b, 3b, b, 4b, 5b, 9b, 3b, b, 4b, 5b, 9b, 3b, ...,$$

die aus der Folge (1) durch Multiplikation mit einem beliebigen Element b aus der Arithmetik modulo 11 hervorgeht.

a) Man suche alle Folgen mit Elementen der Arithmetik modulo 11, die gleichzeitig geometrische Folgen und Fibonaccische Folgen sind.

b) Man beweise, dass es in der Arithmetik modulo 7 keine derartigen Folgen gibt.

67. Die Folge F_{11}^0

$$0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, ...$$

ist in die Summe zweier Fibonaccischer Folgen zu zerlegen, die gleichzeitig geometrische Folgen sind.[23]

68. Man beweise:[24]
a) Lässt sich $\sqrt{5}$ in der Arithmetik modulo p nicht ziehen, so kann in dieser Arithmetik keine Folge konstruiert werden, die gleichzeitig geometrische Folge und F-Folge ist.
b) Lässt sich $\sqrt{5}$ in einer Arithmetik modulo p ziehen, so existieren in dieser Arithmetik F-Folgen, die gleichzeitig geometrische Folgen sind, und jede beliebige Fibonaccische Folge lässt sich als Summe zweier solcher Folgen darstellen.

69. Lässt sich $\sqrt{5}$ in einer Arithmetik modulo p ziehen und ist

$$v_0, v_1, v_2, ..., v_n, ...$$

eine beliebige Fibonaccische Folge dieser Arithmetik, so gilt

$$v_{p-1} = v_0, v_p = v_1, v_{p+1} = v_2, ..., v_{k+p-1} = v_k, ...$$

70. Lässt sich $\sqrt{5}$ in einer Arithmetik modulo p ziehen, so ist die Anzahl der Elemente jeder Fibonaccischen Kreisfolge ohne Wiederholungen ein Teiler der Zahl $p - 1$.

[23] Das heißt, man bestimme zwei Folgen $b_0, b_1, b_2, ..., b_n, ...$ und $b'_0, b'_1, b'_2, ..., b'_n, ...$ die gleichzeitig geometrische und Fibonaccische Folgen sind, für welche

$$c_0 = b_0 + b'_0, c_1 = b_1 + b'_1, c_2 = b_2 + b'_2, ...c_n = b_n + b'_n, ...$$

gilt.

[24] In den Aufgaben 68-70 bezeichnet p eine von 2 und 5 verschiedene Primzahl.

3.1.5 F_p-Folgen

Es sei

$$v_0, v_1, v_2, ..., v_n, ...$$

eine beliebige F_p-Folge. Wir bilden die Folge

$$t_1 = \frac{v_1}{v_0}, t_2 = \frac{v_2}{v_1}, ..., t_n = \frac{v_n}{v_{n-1}}, ...$$

Diese Folge nennen wir Quotientenfolge der Folge $v_0, v_1, v_2, ..., v_n, ...$ Sind einige der Zahlen $v_0, v_1, v_2, ..., v_n, ...$ gleich Null, so enthält die Quotientenfolge außer Zahlen der Arithmetik modulo p das Symbol ∞ (sind irgend zwei benachbarte Elemente der Folge $v_0, v_1, v_2, ..., v_n, ...$ gleich Null, so sind alle Elemente dieser Folge gleich Null; diesen Fall schließen wir aus den Betrachtungen aus).

71. Man berechne die ersten 15 Glieder der Quotientenfolgen, die den Folgen

$$F_2^0, F_3^0, F_5^0, F_7^02, F_{11}^0, F_{13}^0$$

entsprechen.

72. a.) Man beweise, dass für aufeinanderfolgende Glieder der Quotientenfolge, die einer beliebigen Fibonaccischen Folge entspricht, die Formel

$$t_n = 1 + \frac{1}{t_{n-1}}$$

gilt. Unter Benutzung dieser Formel beweise man, dass die Folge $t_1, t_2, ..., t_n, ...$ periodisch ist und im Verlaufe einer ganzen Periode keine Zahl zweimal auftritt.
b) Aus Aufgabe 9.) leite man ab, dass für jede Primzahl p die Fibonaccische Folge

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...$$

unendlich viele Zahlen enthält, die durch p teilbar sind, und dass alle diese Zahlen den gleichen Abstand voneinander haben.

73. Es seien

$$v_0, v_1, v_2, ... \qquad \text{und} \qquad v_0', v_1', v_2', ...$$

zwei beliebige F_p-Folgen und

$$t_1 = \frac{v_1}{v_0}, t_2 = \frac{v_2}{v_1}, ..., t_n = \frac{v_n}{v_{n-1}}, ... \qquad , \qquad t_1' = \frac{v_1'}{v_0'}, t_2' = \frac{v_2'}{v_1'}, ..., t_n' = \frac{v_n'}{v_{n-1}'}, ... \tag{2,3}$$

die ihnen entsprechenden Quotientenfolgen. Man beweise:
Haben (2) und (3) auch nur ein Element gemeinsam (d.h., gilt für irgendwelche k und l die Gleichung $t_k = t_l$), so bestehen sie aus den gleichen Elementen, d.h., jedes Element aus (2) kommt in (3) vor, und umgekehrt.

74. Es seien

$$t_1 = \frac{v_1}{v_0}, t_2 = \frac{v_2}{v_1}, ..., t_n = \frac{v_n}{v_{n-1}}, ... \qquad , \qquad t'_1 = \frac{v'_1}{v'_0}, t'_2 = \frac{v'_2}{v'_1}, ..., t'_n = \frac{v'_n}{v'_{n-1}}, ... \tag{4,5}$$

Quotientenfolgen, die zwei beliebigen F_p-Folgen entsprechen. Man beweise:
Genügen weder t_1 noch t'_1 der Gleichung $x^2 - x - 1 = 0$, so haben (4) und (5) die gleiche Periodenlänge.

Hinweis. Man betrachte die Quotientenfolge

$$\bar{t}_1 = \frac{c_1}{c_0} = \infty, \bar{t}_2 = \frac{c_2}{c_1} = 1, ... \tag{6}$$

die der Folge $c_0 = 0$, $c_1 = 1$, $c_2 = 1$, ... entspricht, und leite daraus die Formel

$$t_{r+1} = \frac{\bar{t}_r + (1 + \bar{t}_r)t_1}{1 + \bar{t}_r t_1}$$

ab, die die Elemente der beliebigen Quotientenfolge (4) durch die Elemente der speziellen Folge (6) ausdrückt.

75. a) Es sei r die Periodenlänge einer Quotientenfolge, die für eine bestimmte F_p-Folge konstruiert worden ist ($p \neq 2$ und $p \neq 5$). Man beweise:
1. Lässt sich $\sqrt{5}$ in der Arithmetik modulo p nicht ziehen, so ist r ein Teiler der Zahl $p + 1$;
2. Lässt sich $\sqrt{5}$ in der Arithmetik modulo p ziehen, so ist $p - 1$ durch r teilbar.

b) Man beweise, dass für alle von 2 und 5 verschiedenen Primzahlen p in der Fibonaccischen Folge

$$a_0 = 0, a_1 = 1, a_2 = 1, a_3 = 2, a_4 = 3, a_5 = 5, a_6 = 8, ...$$

der gewöhnlichen Arithmetik entweder a_{p+1} oder a_{p-1} durch p teilbar ist. Der erste Fall tritt ein, wenn sich $\sqrt{5}$ in der Arithmetik modulo p nicht ziehen lässt, der zweite[25], wenn $\sqrt{5}$ bestimmt werden kann (vergleiche mit Aufgabe 69).

3.2 Das Pascalsche Dreieck

Unter dem Pascalschen Dreieck versteht man folgende unendliche Zahlentafel:

				1						
			1		1					
		1		2		1				
	1		3		3		1			
1		4		6		4		1		
1	5		10		10		5		1	

[25] Man kann beweisen, dass sich $\sqrt{5}$ in der Arithmetik modulo p ($p \neq 2$ und $p \neq 5$) denn und nur dann ziehen lässt, wenn p die Form $5k \pm 1$ hat.

Jede Zahl dieser Tafel ist gleich der Summe der beiden Zahlen, die rechts und links über ihr stehen. Das Pascalsche Dreieck ist symmetrisch bezüglich seiner Mittelsenkrechten. Wir nummerieren die Zeilen des Pascalschen Dreiecks wie folgt:

			1			nullte Zeile
		1		1		erste Zeile
	1		2		1	zweite Zeile

Die Zahl des Pascalschen Dreiecks, die in der n-ten Zeile und auf dem k-ten Platz von links, vom nullten aus gezählt, steht, wird gewöhnlich mit C_n^k bezeichnet (beispielsweise ist $C_5^2 = 10$). Nach Definition des Pascalschen Dreiecks ist

$$C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$$

(wir benutzen zunächst nicht, dass es sich um die Binomialkoeffizienten handelt; Anm. d. Red.).
Dementsprechend kann das Pascalsche Dreieck in der Form

				C_0^0				
			C_1^0			C_1^1		
		C_2^0			C_2^1			C_2^2	
	C_3^0			C_3^1			C_3^2			C_3^3

geschrieben werden. Aus der Symmetrie folgt $C_n^k = C_n^{n-k}$.

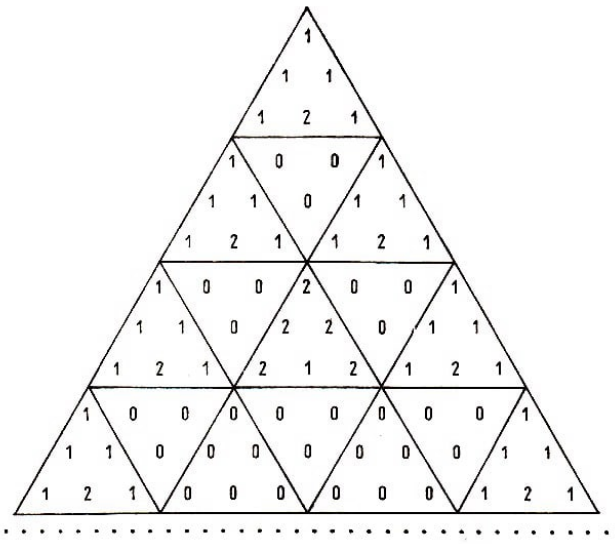
Wir untersuchen jetzt die Teilbarkeit der Zahlen des Pascalschen Dreiecks.
Zu diesem Zweck betrachten wir ein Pascalsches Dreieck in einer Arithmetik modulo m, das sich von dem bisherigen nur dadurch unterscheidet, dass seine Zahlen Elemente der Arithmetik modulo m sind. Für $m = 6$ hat dieses Pascalsche Dreieck beispielsweise die Form

					1						
				1		1					
			1		2		1				
		1		3		3		1			
	1		4		0		4		1		
1		5		4		4		5		1	
1	0		3		2		3		0		1

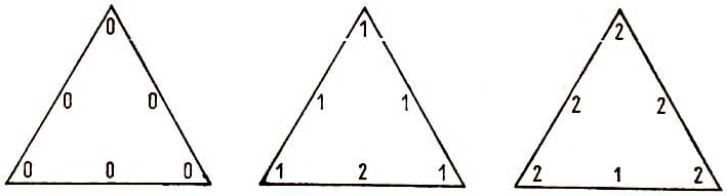
Die Zahlen des modulo m reduzierten Pascalschen Dreiecks wollen wir mit P_n^k bezeichnen, wobei P_n^k der Rest von C_n^k bei der Division durch m ist.

76. Man beweise, dass in der n-ten Zeile des modulo 2 reduzierten Pascalschen Dreiecks alle Zahlen außer denen am Rande (der nullten und n-ten Zahl) dann und nur dann gleich Null sind, wenn $n = 2^k$ ist.

Wir stellen das Pascalsche Dreieck für die Arithmetik modulo 3 auf (siehe S. 115 oben).



Wir sehen, dass es (zumindest in den Teilen, die auf dem Schema zu sehen sind) aus drei verschiedenen Typen von Dreiecken besteht, deren Spitze nach oben gerichtet ist:



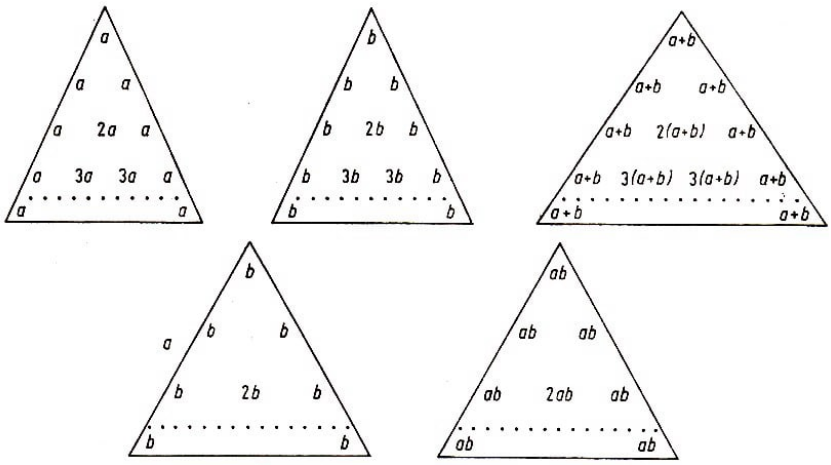
Diese Dreiecke wollen wir Elementardreiecke nennen), und außerdem aus Dreiecken mit nach unten gerichteter Spitze, die jedoch nur Nullen enthalten und uns hier nicht interessieren.
Für diese Elementardreiecke kann man in natürlicher Weise eine Addition einführen. Die Summe von Dreiecken ist das Dreieck, dessen Zahlen die Summe der entsprechenden Zahlen aus den zu addierenden Dreiecken sind. Danach ist, wie aus dem Schema ersichtlich, jedes Elementardreieck die Summe der beiden schräg über ihm stehenden Elementardreiecke.

Das modulo 3 reduzierte Pascalsche Dreieck setzt sich also aus Elementardreiecken auf dieselbe Weise wie aus Zahlen zusammen. Diese Tatsache, die eine bestimmte Periodizität in der Struktur des Pascalschen Dreiecks zum Ausdruck bringt, gilt allgemein, d.h. in jeder beliebigen Arithmetik modulo m. In Aufgabe 77 wird sie genauer formuliert (siehe unten).

Wir verallgemeinern etwas den Begriff des Pascalschen Dreiecks, und zwar betrachten wir solche Dreiecke, bei denen an den beiden Seiten nicht die Zahl 1 steht, sondern eine beliebige Zahl a:

a
a a
a 2a a
a 3a 3a a ...

Ein derartiges Dreieck erhält man aus dem gewöhnlichen Pascalschen Dreieck durch Multiplikation aller seiner Zahlen mit der Zahl a.
Im folgenden wird uns nicht mehr das gesamte Dreieck interessieren, sondern nur der Teil oberhalb einer bestimmten Zeile. Solche Dreiecke (mit gleicher Zeilenzahl) kann man addieren und mit Zahlen multiplizieren:



77. Alle Zahlen der s-ten Zeile eines modulo m reduzierten Pascalschen Dreiecks - mit Ausnahmen der äußeren - seien Nullen. Man beweise, dass das Dreieck in diesem Falle die in Abb. 3.8 dargestellte Form hat.

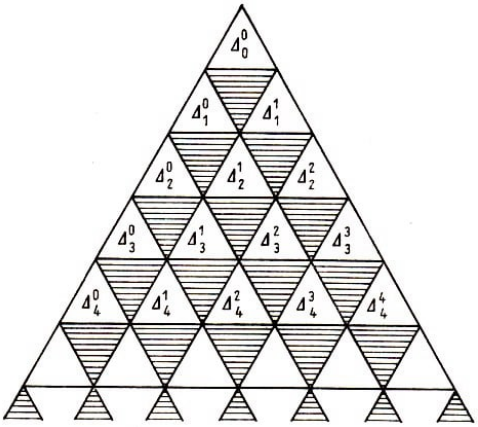


Abb. B.8

Jedes der Dreiecke $\triangle_n^k$, in die das Ausgangsdreieck zerlegt ist, besteht aus s Zeilen. Die schraffierten Dreiecke enthalten nur Nullen. Die Dreiecke $\triangle_n^k$ genügen folgenden Gleichungen:

a) $\triangle_n^{k-1} + \triangle_n^k = \triangle_{n+1}^k$
b) $\triangle_n^k = P_n^k \cdot \triangle_0^0$

78. In der s-ten Zeile eines modulo m reduzierten Pascalschen Dreiecks seien alle Zahlen außer den äußeren Nullen. Man beweise, dass die Zeilen der Nummern $s^2, s^3, ..., s^k, ...$ die gleiche Eigenschaft haben.

79. Erhebt man das Binom $1 + x$ in die n-te Potenz und ordnet es nach wachsenden Potenzen von x, so erhält man die Identität

$$(1 + x)^n = C_n^0 + C_n^1 x + C_n^2 x^2 + ... + C_n^n x^n$$

oder, modulo m gerechnet,

$$(1+x)^n = P_n^0 + P_n^1 x + P_n^2 x^2 + ... + P_n^n x^n$$

80. Man beweise, dass in der Arithmetik modulo p alle p-ten Zeilen des Pascalschen Dreiecks (außer den äußeren Zahlen) aus Nullen bestehen. (Daraus folgt auf Grund der Aufgabe 78, dass die Zeilen der Nummern $p^2, p^3, ..., p^k, ...$ die gleiche Eigenschaft haben.)

3.3 Gebrochene lineare Funktionen

Der Term $ax+b$, wobei a und b irgendwelche Zahlen sind, definiert eine lineare Funktion von x. Beispiele sind:

$$5x+3, \qquad x+1, \qquad \frac{3}{4}x, \qquad x$$

Der Quotient zweier linearer Funktionen heißt gebrochene lineare Funktion. Beispiele sind:

$$\frac{5x+3}{\frac{3}{4}x+5}, \qquad \frac{x}{x+1}, \qquad \frac{4x+6}{14x+2}$$

er allgemeine Term einer gebrochenen linearen Funktion ist

$$\frac{ax+b}{cx+d}$$

Eine gebrochene lineare Funktion wollen wir mit $f(x)$ bezeichnen. Wird in einer gebrochenen linearen Funktion $f(x)$ an Stelle von x eine Zahl n gesetzt, so erhält man die Zahl $\frac{an+b}{cn+d}$ die man mit $f(n)$ bezeichnet. Die lineare Funktion ist ein Spezialfall der gebrochenen linearen Funktion:

$$ax+b = \frac{ax+b}{0 \cdot x+1}$$

Wir wollen nun lineare und gebrochene Funktionen modulo p betrachten, d.h. nur Zahlen einer Arithmetik modulo p benutzen und die Ergebnisse der Addition, Subtraktion, Multiplikation und Division modulo p auffassen.
Setzen wir in der linearen Funktion $ax+b$ an Stelle von x eine Zahl n aus der Arithmetik modulo p ein, so liegt die Zahl $an+b$ wieder in dieser Arithmetik. Somit ordnet eine lineare Funktion jeder Zahl aus einer Arithmetik modulo p wieder eine Zahl derselben Arithmetik zu.
Für die lineare Funktion $f(x) = 7x+4$ erhalten wir beispielsweise in der Arithmetik modulo 11:

$$f(0) = 4; f(1) = 0; f(2) = 7; f(3) = 3; f(4) = 10;$$
$$f(5) = 6; f(6) = 2; f(7) = 9; f(8) = 5; f(9) = 1; f(10) = 8$$

Dies kann in Form einer Tabelle

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 0 & 7 & 3 & 10 & 6 & 2 & 9 & 5 & 1 & 8 \end{pmatrix}$$

geschrieben werden, wobei in der oberen Zeile alle für x eingesetzten Zahlen und in der unteren die Funktionswerte stehen. Statt einer Tabelle kann man auch das Schema der Abb. B.9 benutzen.

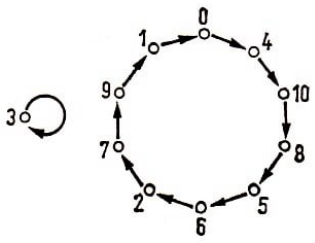


Abb. B.9

Die Pfeile zeigen an, in welche Zahl jede der Zahlen der Arithmetik modulo 11 durch die Funktion über- geführt wird. Aus dem Schema ist ersichtlich, dass die Funktion $7x + 4$ in der Arithmetik modulo 11 die Zahl 3 fest lässt (3 heißt Fixpunkt); die anderen Zahlen bilden einen Zyklus.

Ein Spezialfall einer linearen Funktion ist uns bereits in Abschnitt 1.2. bei der Betrachtung der Multiplikation mit der Zahl ax begegnet, nämlich die lineare Funktion ax.
Durch Wiederholung der dort angestellten Überlegungen kann man sich leicht davon überzeugen, dass auch das Schema einer willkürlich gewählten linearen Funktion in Zyklen zerfällt, die alle, mit Ausnahme der Fixpunkte, die gleiche Länge haben. Wir werden darauf noch zurückkommen, wenn wir diese Frage für gebrochene lineare Funktionen behandeln.

Wir untersuchen jetzt eine beliebige gebrochene lineare Funktion

$$\frac{ax + b}{cx + d}$$

Aus $ad = bc$ folgt

$$\frac{ax + b}{cx + d} = \frac{a}{c}\frac{c(ax + b)}{a(cx + d)} = \frac{a}{c}\frac{cax + cb}{acx + ac} = \frac{a}{c}$$

somit ist der Term $\frac{ax+b}{cx+d}$ für $ad = cb$ von x unabhängig. Wir werden deshalb immer $ad \neq bc$ voraussetzen.

Wenn wir in eine gebrochene lineare Funktion für das Argument Zahlen aus einer Arithmetik modulo p einsetzen, ist es nicht sicher, dass wir stets wieder Zahlen aus diesem System erhalten.
Tatsächlich kann durch Einsetzen einer Zahl n in die Funktion $\frac{ax+b}{cx+d}$ der Nenner $cn + d$ Null werden, wodurch wir für die Funktion den Ausdruck $\frac{an+b}{0}$ erhalten (aus der Bedingung $ad \neq bc$ folgt, dass dann $an + b \neq 0$ ist).

Die Division durch 0 ist jedoch auch in einer Arithmetik modulo p nicht möglich. Wir wollen deshalb die Arithmetik modulo p erweitern, indem wir das Symbol ∞ einführen[26] und vereinbaren, dann ∞ als Wert unserer Funktion anzusehen.
Schließlich verabreden wir noch, für $x = \infty$ die Zahl $\frac{a}{c}$ als Wert der gebrochenen linearen Funktion anzusehen, d.h., wir setzen $f(\infty) = \frac{a}{c}$.[27]
Die so definierte gebrochene lineare Funktion ordnet dann wieder jedem der $(p+1)$ Elemente $0, 1, ..., p-1, \infty$ eines dieser Elemente zu. Beispielsweise nimmt die gebrochene lineare Funktion $f(x) = \frac{x+2}{x+1}$ in der Arithmetik modulo 7 die Werte

$$f(0) = 2, f(1) = 5, f(2) = 6, f(3) = 3, f(4) = 4, f(5) = 0, f(6) = \infty, f(\infty) = 1$$

an. Dies kann wieder in Form einer Tabelle

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \\ 2 & 5 & 6 & 3 & 4 & 0 & \infty & 1 \end{pmatrix}$$

oder in Form eines Schemas (Abb. 3.10) geschrieben werden.

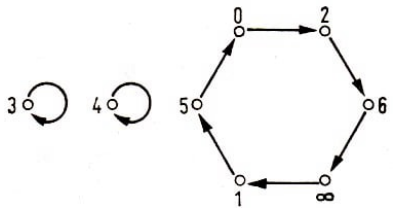


Abb. B.10

Aus diesem Schema ist ersichtlich, dass die gebrochene lineare Funktion $f(x) = \frac{x+2}{x+1}$ in der Arithmetik modulo 7 die beiden Fixpunkte 3 und 4 hat; alle anderen Zahlen bilden einen einzigen Zyklus.

81. Man stelle die Schemata der gebrochenen linearen Funktionen

$$\frac{4x+1}{2x+3}, \qquad \frac{2x+1}{3x+2}, \qquad \frac{3x-1}{x+1}$$

in der Arithmetik modulo 7 auf.

Wir betrachten nun die beiden gebrochenen linearen Funktionen

$$f(x) = \frac{ax+b}{cx+d} \qquad \text{und} \qquad g(x) = \frac{-dx+b}{cx-a}$$

Man sieht sofort: Führt $f(x)$ die Zahl m in die Zahl n über, d.h., ist $f(m) = n$, so führt $g(x)$ die Zahl n wieder in die Zahl m zurück, d.h., $g(n) = m$. Man erhält das Schema

[26] Wir weisen nochmals darauf hin, dass das Symbol ∞ keine Zahl ist und man daher mit ihm nicht wie mit einer Zahl rechnen kann. Die Fälle, in denen wir auf das Symbol ∞ treffen, werden wir stets gesondert betrachten.

[27] Es liegt nahe, $\frac{a}{\infty} = 0$ zu setzen. Daher ist

$$f(x) = \frac{ax+b}{cx+d} = \frac{a+\frac{b}{x}}{c+\frac{d}{x}} \qquad \text{also} \qquad f(\infty) = \frac{a+\frac{b}{\infty}}{c+\frac{d}{\infty}} = \frac{a+0}{c+0} = \frac{a}{c}$$

der Funktion $g(x)$ aus dem Schema der Funktion $f(x)$, indem man die Richtung aller Pfeile umkehrt.

Diese Funktion $g(x)$ heißt invers zu $f(x)$ (andererseits ist $f(x)$ invers zu $g(x)$). Die zu $f(x)$ inverse Funktion werden wir künftig mit $f^{-1}(x)$ bezeichnen.

82. Es sei $f(x) = \frac{ax+b}{cx+d}$ eine beliebige gebrochene lineare Funktion. Man beweise, dass in ihrem Schema zu jeder Zahl ein und nur ein Pfeil führt.

83. Man beweise, dass das Schema einer gebrochenen linearen Funktion stets in Zyklen zerfällt und jede Zahl des Schemas in einem und nur einem Zyklus vorkommt (vgl. Aufgabe 15).

84. Führt eine gebrochene lineare Funktion drei Zahlen in sich über, dann werden alle Zahlen ohne Ausnahme in sich übergeführt.

Bei der Untersuchung einer gebrochenen linearen Funktion ist für uns die Zuordnung, welche sie zwischen den Zahlen der Arithmetik modulo p herstellt, wesentlich, d.h. ihre Tabelle oder ihr Schema. Die algebraische Gestalt der Funktion ist dabei belanglos.
Ein und dieselbe gebrochene lineare Funktion kann man in verschiedener Gestalt darstellen: Multipliziert man Zähler und Nenner eines solchen Ausdruckes mit einer beliebigen Zahl, so wird man stets eine andere, von der ersten verschiedene Gestalt der Funktion erhalten. Die Ausdrücke

$$\frac{2x+1}{7x+5} \qquad \text{und} \qquad \frac{7x-2}{8x+1}$$

sind beispielsweise Formen ein und derselben gebrochenen linearen Funktion in der Arithmetik modulo 11 (man kann sich davon leicht überzeugen, wenn man die entsprechenden Tabellen aufschreibt).

Es seien die beiden gebrochenen linearen Funktionen

$$f(x) = \frac{ax+b}{cx+d} \qquad \text{und} \qquad g(x) = \frac{a'x+b'}{c'x+d'}$$

gegeben. Wir bilden eine neue gebrochene lineare Funktion, indem wir in $f(x)$ für x die Funktion $g(x)$ einsetzen:

$$f(g(x)) = \frac{a\frac{a'x+b'}{c'x+d'} + b}{c\frac{a'x+b'}{c'x+d'} + d} = \frac{(aa'+bc')x + ab' + bd'}{(ca'+dc')x + cb' + dd'}$$

85. Man berechne in der Arithmetik modulo 7 aus den beiden gegebenen Funktionen

$$f(x) = \frac{x+5}{5x+1} \qquad \text{und} \qquad g(x) = \frac{4x+3}{6x+3}$$

die Funktionen $f(g(x))$ und $g(f(x))$.

86. Man gebe in der Arithmetik modulo 7 eine gebrochene lineare Funktion an derart, dass $f(0) = 0$, $f(1) = 4$ und $f(4) = 2$ ist.

87. Gegeben seien drei verschiedene Zahlen x_1, x_2 und x_3. Man gebe eine gebrochene

lineare Funktion an derart, dass $f(x_1) = 0$, $f(x_2) = 1$, $f(x_3) = \infty$ ist.

88. Gegeben seien drei verschiedene Zahlen y_1, y_2 und y_3. Man beweise, dass stets eine gebrochene lineare Funktion $f(x)$ existiert, die der Bedingung $f(0) = y_1$, $f(1) = y_2$ und $f(\infty) = y_3$ genügt.

89. Es seien drei Zahlenpaare (x_1, y_1), (x_2, y_2) und (x_3, y_3) gegeben. Man beweise, dass stets eine und nur eine gebrochene lineare Funktion gefunden werden kann derart, dass $f(x_1) = y_1$, $f(x_2) = y_2$, $f(x_3) = y_3$ ist.

90. Man bestimme die Anzahl aller verschiedenen gebrochenen linearen Funktionen in einer Arithmetik modulo p.

Die Funktion $f(f(x))$ bezeichnen wir mit $f^2(x)$. Analog führen wir die gebrochenen linearen Funktionen $f^3(x)$, $f^4(x)$, ..., $f^n(x)$ ein:

$$f^3(x) = f(f^2(x)), \qquad f^4(x) = f(f^3(x)), \qquad ..., \qquad f^(x) = f(f^{n-1}(x))$$

Zum Beispiel:

$$f(x) = \frac{x+1}{x},$$
$$f^2(x) = \frac{\frac{x+1}{x} + 1}{\frac{x+1}{x}} = \frac{2x+1}{x+1},$$
$$f^3(x) = \frac{\frac{2x+1}{x+1} + 1}{\frac{2x+1}{x+1}} = \frac{3x+2}{2x+1}$$

Die durch die Funktionen $f^n(x)$ vermittelten Transformationen gehen aus dem Schema der Funktion $f(x)$ hervor. Die Funktion $f(x)$ bewirkt, dass jeder Punkt ihres Schemas in den folgenden übergeführt, d.h. in Pfeilrichtung um einen Schritt bewegt wird.
Bei Anwendung der Funktion $f^2(x)$ wird jeder Punkt im Schema von $f(x)$ um zwei Stellen weitergeführt, er kommt an die übernächste Stelle.

Allgemein wird jeder Punkt durch die Anwendung der Funktion $f^n(x)$ auf das Schema von $f(x)$ in seinem Zyklus um n Stellen weitergeführt, nämlich in Pfeilrichtung über $n-1$ Punkte hinweg zur n-ten Stelle.
Somit kann man die Schemata für die Funktionen $f^2(x)$, $f^3(x)$, ... aus dem Schema der Funktion $f(x)$ ohne jede Rechnung ablesen.

91. Gegeben sei

$$f(x) = \frac{3x-1}{x+1}$$

Man konstruiere die Schemata für die Funktionen $f^2(x), f^3(x), f^4(x)$ in der Arithmetik modulo 7.

92. Gegeben sei die Zahl x_0 in dem Schema der Funktion $f(x)$ in einem Zyklus der Länge s. Man beweise, dass $f^k(x_0) = x_0$, falls k durch s teilbar ist. Umgekehrt, ist $f^k(x_0) = x_0$, so ist k durch s teilbar.

93. Gegeben sei eine beliebige gebrochene lineare Funktion $f(x)$ in einer Arithmetik modulo p. Man beweise:
Hat eine der Funktionen $f^2(x)$, $f^3(x)$, ..., $f^n(x)$ einen Fixpunkt, der kein Fixpunkt von $f(x)$ ist, so lässt diese Funktion alle Punkte fest.

94. Gegeben sei eine beliebige gebrochene lineare Funktion $f(x)$ in einer Arithmetik modulo p. Man beweise, dass die Zyklen, aus denen ihr Schema besteht, alle die gleiche Länge haben (dabei sind die Zyklen, die nur aus einer Zahl bestehen, d.h. Fixpunkte von $f(x)$, nicht mitzuzählen). (Vgl. Aufgabe 15)

95. Gegeben sei in einer Arithmetik modulo p die Folge

$$x_0, x_1 = f(x_0) = \frac{ax_0 + b}{cx_0 + d}, \qquad x_2 = f(x_1) = \frac{ax_1 + b}{cx_1 + d},$$
$$..., \qquad x_k = f(x_{k-1}) = \frac{ax_{k-1} + b}{cx_{k-1} + d}, ...$$

(oder, was das gleiche ist, $x_k = f^k(x_0)$). Man beweise:

1. Lässt sich $\sqrt{(a-d)^2 + 4bc}$ in der Arithmetik modulo p nicht ziehen, so gilt $x_{p+1} = x_0$.
2. Aus $(a-d)^2 + 4bc = 0$ folgt $x_p = x_0$.
3. Ist $(a-d)^2 + 4bc \neq 0$ und lässt sich $\sqrt{(a-d)^2 + 4bc}$ in der Arithmetik modulo p ziehen, so gilt $x_{p-1} = x_0$.

96. Man berechne die Funktionen $f^2(x)$ und $f^3(x)$ für die Funktion $f(x) = \frac{x-3}{x+1}$ in der Arithmetik modulo p. Wie lang sind die Zyklen von $f(x)$?
Man zeige, dass ein Zyklus der Länge 3 existiert.

97. a) Es sei p eine Primzahl größer als 3. Man beweise, dass sich $\sqrt{3}$ in der Arithmetik modulo p dann und nur dann ziehen lässt, wenn p die Form $3k + 1$ hat.

b) Man beweise, dass für jede ganze Zahl a alle Primfaktoren der Zahl $a^2 + 3$, die größer als 3 sind, die Form $3k + 1$ haben. Umgekehrt kann für jede Primzahl p der Form $3k + 1$ ein a gefunden werden derart, dass $a^2 + 3$ durch p teilbar ist.

98. Für die Funktion

$$f(x) = \frac{x-1}{x+1}$$

berechne man die Funktionen $f^2(x)$, $f^3(x)$ und $f^4(x)$ in einer Arithmetik modulo p. Wie lang sind ihre Zyklen? Man zeige, dass ein Zyklus mit der Länge 4 existiert.

99. a) Gegeben sei eine Primzahl p größer als 2. Man beweise, dass sich $\sqrt{-1}$ genau dann in der Arithmetik modulo p ziehen lässt, wenn $p = 4k + 1$ gilt.
b) Man beweise, dass für jede ganze Zahl a alle ungeraden Primfaktoren der Zahl a^2+1 die Form $4k+1$ haben. Jede Primzahl der Form $4k+1$ tritt in der Primfaktorenzerlegung mindestens einer Zahl $a^2 + 1$ auf.

4 Ergänzungen zur Fibonaccischen Folge und zum Pascalschen Dreieck

4.1 Die Anwendung der p-adischen Zahlen auf die Fibonaccische Folge

Es wurde schon gezeigt, dass in einer Arithmetik modulo einer Primzahl p das Problem der Teilbarkeit der Zahlen einer Fibonaccischen Folge[28] durch p leicht lösbar ist durch Zurückführung dieser Folge auf eine geometrische Progression, wenn sich $\sqrt{5}$ dieser Arithmetik modulo p ziehen lässt.
Wir zeigen jetzt, dass durch die gleiche Überlegung Zahlen in der Fibonaccischen Folge ermittelt werden können, welche durch beliebige Potenzen p^k teilbar sind, wenn wir an Stelle der Arithmetik modulo p die p-adischen Zahlen benutzen.

Eine Folge p-adischer Zahlen

$$u_0, u_1, u_2, ..., u_n, ...$$

heißt Fibonaccische Folge, wenn für $n \geq 2$

$$u_n = u_{n-2} + u_{n-1}$$

gilt.

100.[29] Man stelle alle p-adischen Fibonaccischen Folgen fest, die gleichzeitig geometrische Progressionen sind. Man beweise, dass solche Folgen dann und nur dann existieren, wenn sich $\sqrt{5}$ in der Arithmetik modulo p ziehen lässt.

101. Es möge sich $\sqrt{5}$ in der Arithmetik modulo p ziehen lassen. Man beweise, dass jede beliebige p-adische F-Folge als Summe zweier geometrischer Progressionen dargestellt werden kann.

102. In einer Arithmetik modulo p lasse sich $\sqrt{5}$ ziehen. Man beweise, dass sich die letzten k Ziffern der Zahlen einer p-adischen F-Folge periodisch wiederholen; die Länge der Periode ist ein Teiler der Zahl $p^{k-1}(p-1)$, so dass die Zahlen mit den Nummern n und $n + p^{k-1}(p-1)$ (die Zahlen u_n und $u_{n+p^{k-1}(p-1)}$ in den letzten k Ziffern übereinstimmen.

103. Lässt sich in einer Arithmetik modulo p die Quadratwurzel aus 5 ziehen, so sind von den gewöhnlichen ganzen Zahlen der F-Folge

$$0, 1, 1, 2, 3, 5, 8, ...$$

die Zahlen mit den Indizes $p^{k-1}(p-1)$ durch p^k teilbar.

[28] Dieses Kapitel enthält zusätzlichen Stoff und kann bei der ersten Lektüre übergangen werden.
[29] In den Aufgaben 100-108 bezeichnet p eine von 2 und 5 verschiedene Primzahl.

4.2 Der Zusammenhang zwischen Pascalschem Dreieck und Fibonaccischer Folge

104. Man beweise, dass die Zahlen des Pascalschen Dreiecks nach der Formel

$$C_n^k = \frac{n!}{k!(n-k)!} \equiv \binom{n}{k}$$

berechnet werden können ($n!$ bezeichnet das Produkt $1 \cdot 2 \cdot 3 \cdot (n-1) \cdot n$; unter dem Symbol $0!$, das eigentlich keinen Sinn hat, ist zweckmäßigerweise der Wert 1 zu verstehen, da sich dann in vielen Formeln Fallunterscheidungen vermeiden lassen).

Für $k < p$ und $n - k < p$ sind die Werte $k!$ und $(n-k)!$ in der Arithmetik modulo p von Null verschieden. Folglich ist in diesem Fall die Division durch $k!(n-k)!$ in der Arithmetik modulo p möglich, und die Formel, die in Aufgabe 104 aufgestellt wurde, behält auch in der Arithmetik modulo p ihre Gültigkeit, d.h., es ist [30]

$$P_n^k = \frac{n!}{k!(n-k)!}$$

105. Man beweise, dass im modulo p reduzierten Pascalschen Dreieck

$$P_{p-1-k}^k = (-1)^k P_{2k}^k \qquad (\text{für } k \leq \frac{p-1}{2})$$

gilt.

106. Man beweise, dass im modulo p reduzierten Pascalschen Dreieck

$$P_{2n}^n = (-4)^n P_{\frac{p-1}{2}}^n \qquad (\text{für } n \leq \frac{p-1}{2})$$

gilt.

Auf der Symmetrieachse des Pascalschen Dreiecks stehen Zahlen der Form $C_{2n}^n (= \binom{2n}{n})$:

$$1, 2, 6, 20, 70, 252, ...$$

Man kann in dem Dreieck auch andere Linien, nämlich die Diagonalen, auszeichnen (siehe Abb. 3.11).

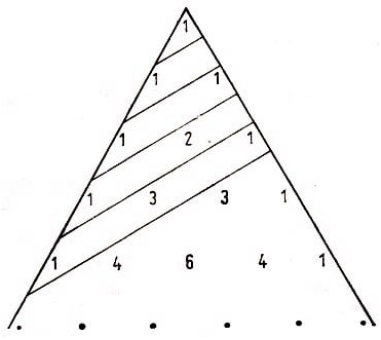


Abb. B.11

[30] Diese Gleichung bedeutet in der Arithmetik modulo p: Alle Operationen auf der rechten Seite sind modulo p aufzufassen. Auch das Symbol $n!$ ist modulo p zu verstehen, d.h., jeder Faktor des Produktes $1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1) \cdot n$ (und damit das Produkt überhaupt) ist durch seinen Rest bei der Division durch p zu ersetzen.

Beispielsweise stehen auf der dritten Diagonale die Zahlen, 1, 1, auf der vierten die Zahlen 1, 2 und allgemein auf der n-ten Diagonale die Zahlen

$$C_{n-1}^0, C_{n-2}^1, ..., C_{n-1-k}^k, ...$$

(sie lassen sich solange fortsetzen, wie das Symbol C_{n-k}^{k-1} sinnvoll ist, d.h. solange $k \leq n-1-k$, also $2k \leq n-1$ oder $k \leq \frac{n-1}{2}$ ist).

Die Aufgabe 105 zeigt, dass die k-te Zahl der p-ten Diagonale eines modulo p reduzierten Dreiecks gleich der mit $(-1)^k$ multiplizierten k-ten Zahl der Symmetrieachse ist. Die Aufgabe 106 zeigt den Zusammenhang zwischen der Symmetrieachse und der $\frac{p-1}{2}$-ten Zeile eines modulo p reduzierten Dreiecks.

Wir multiplizieren die Zahlen, die auf der Symmetrieachse eines modulo p reduzierten Pascalschen Dreiecks stehen, mit den Zahlen einer beliebigen geometrischen Progression $1, q, q^2, ...$ und addieren die ersten $\frac{p+1}{2}$ Zahlen der so konstruierten Folge. Wir erhalten dann die Summe

$$S = 1 + 2q + ... + P_{2n}^n q^n + ... + P_{p-1}^{\frac{p-1}{2}} q^{\frac{p-1}{2}}$$

107. Man beweise, dass die Summe

$$S = 1 + 2q + ... + P_{2n}^n q^n + ... + P_{p-1}^{\frac{p-1}{2}} q^{\frac{p-1}{2}}$$

in der Arithmetik modulo p gleich 0, gleich $+1$ oder gleich -1 ist, und zwar 0 nur dann, wenn $q = \frac{1}{4}$ ist.

Wir zeigen jetzt einen Zusammenhang zwischen dem Pascalschen Dreieck und der Fibonaccischen Folge. Abgesehen davon, dass er an und für sich interessant ist, führt uns dieser Zusammenhang zu einer neuen Eigenschaft der Fibonaccischen Folge.

108. Es sei b_n die Summe aller der Zahlen, die auf der n-ten Diagonale des Pascalschen Dreiecks stehen. Man zeige, dass $b_n = a_n$ gilt, wobei a_n die n-te Zahl der Fibonaccischen Folge

$$a_0 = 0, \quad a_1 = 1, \quad a_2 = 1, \quad a_3 = 2, \quad ...$$

ist.

109. Man suche einen Ausdruck für die p-te Zahl der F_p-Folge (man beweise, dass $c_p = 5^{\frac{p-1}{2}}$ ist).

Aus der Aufgabe 109 folgt $c_p = 1$, wenn sich $\sqrt{5}$ in der Arithmetik modulo p ziehen lässt, andernfalls ist $c_p = -1$ (siehe Aufgabe 85).
Im ersten Fall ist, wie wir aus Aufgabe 75b) wissen, $c_{p-1} = 0$; bei den Fibonaccischen Folgen mit den Gliedern $c_0 = 0$, $c_1 = 1$, $c_2 = 1$, ... und c_{p-1}, c_p, c_{p+1} stimmen die ersten beiden Glieder überein; dann stimmen aber diese Folgen überhaupt überein, d.h. $c_{p-1+k} = c_k$.
Die Länge der Periode ist in diesem Fall ein Teiler der Zahl $p-1$.

Im zweiten Fall ist $c_{p+1} = 0$ und $c_{p+2} = c_p + c_{p+1} = -1$; die ersten beiden Glieder

der beiden Fibonaccischen Folgen $c_0 = 0$, $c_1 = 1$, $c_2 = 1$, ... und c_{p+1}, c_{p+2}, c_{p+3} unterscheiden sich um den Faktor -1; somit erhält man die zweite Folge aus der ersten, wenn man diese mit -1 multipliziert: $c_{p+1+k} = -c_k$, woraus $c_{2p+2} = 0$ und $c_{2p+3} = -c_{p+2} = 1$ folgt.
Die Länge der Periode ist in diesem Fall ein Teiler der Zahl $2p + 2$.

Wir zeigen eine weitere Anwendung der Beziehungen zwischen Pascalschem Dreieck und Fibonaccischer Folge.

110. Es seien n beliebige Zahlen $d_0, ..., d_{n-1}$ gegeben. Wir bilden die Summen

$$d_0^{(1)} = d_0 + d_1, \quad d_1^{(1)} = d_1 + d_2, \quad ..., \quad d_{n-2}^{(1)} = d_{n-2} + d_{n-1}$$

Damit haben wir die $n-1$ Zahlen $d_0^{(1)}, d_1^{(1)}, ..., d_{n-2}^{(1)}$ erhalten. Wir setzen diesen Prozess fort:

$$d_0^{(2)} = d_0^{(1)} + d_1^{(1)}, \qquad ..., \qquad d_{n-3}^{(2)} = d_{n-3}^{(1)} + d_{n-2}^{(1)}$$

Wir erhalten eine dreieckige Tabelle:

$$\begin{array}{ccccccccccc}
d_0 & & d_1 & & d_2 & ... & d_{n-3} & & d_{n-2} & & d_{n-1} \\
& d_0^{(1)} & & d_1^{(1)} & & ... & & d_{n-3}^{(1)} & & d_{n-2}^{(1)} & \\
& & d_0^{(2)} & & & ... & & & d_{n-3}^{(2)} & & \\
& & & & & ... & & & & & \\
& & & & & d_0^{(n-1)} & & & & &
\end{array}$$

Man beweise die Beziehung

$$d_0^{(n-1)} = C_{n-1}^0 d_0 + C_{n-1}^1 d_1 + ... + C_{n-1}^{n-1} d_{n-1}$$

111. Man zeige, dass die Quadratsumme der Zeilen eines Pascalschen Dreiecks wieder eine Zahl des Pascalschen Dreiecks ist.

112. Man beweise, dass in jeder modulo p reduzierten F-Folge

$$v_0, v_1, v_2, ..., v_n, ...$$

die Gleichung

$$v_k = v_{k+p} + v_{k+2p} \qquad \text{(für jedes } k\text{)}$$

gilt.

113. Man beweise, dass die Zahlen einer F_p-Folge, deren Indizes durch p teilbar sind, wieder eine F_p-Folge bilden.

4.3 Zahlen der Fibonaccischen Folge, die durch gegebene Zahlen teilbar sind

Wir betrachten nun die Verteilung der Zahlen einer Fibonaccischen Folge, die durch eine beliebige Zahl m teilbar sind.

114. Es seien a und b ganze Zahlen. Man beweise, dass

$$(a+b)^m = a^m + ma^{m-1}b + b^2S$$

gilt, wobei S eine gewisse ganze Zahl ist.

115. Ist die k-te Zahl a_k einer Fibonaccischen Folge durch d teilbar, so ist jede der Differenzen

$$a_{kl-1} - a_{k-1}^l \qquad , \qquad a_{kl+1} - a_{k+1}^l$$

für jedes l durch d^2 teilbar. Hinweis. Man benutze die Aufgaben 52 und 63.

116. Ist a_k teilbar durch m^n, so ist die Differenz $a_{k+1}^m - a_{k-1}^m$ durch m^{n+1} teilbar.

117. Ist a_k durch m^n teilbar, so ist a_{km} durch m^{n+1} teilbar.

118. Ist a_k durch m teilbar, so sind alle Zahlen mit den Nummern $km^{n-1}s$ (für jedes s) durch m^n teilbar (vgl. mit Aufgabe 68.

Die Aufgabe 118 gestattet uns, in der Fibonaccischen Folge Zahlen zu finden, die durch eine beliebige Potenz einer gegebenen Primzahl p teilbar sind. Ist p von 2 und 5 verschieden, so können wir das Resultat von Aufgabe 75 b) anwenden:

Lässt sich $\sqrt{5}$ in der Arithmetik modulo p ziehen, so ist a_{p-1} durch p teilbar; zufolge Aufgabe 118 sind daher alle Zahlen der Form $a_{(p-1)p^{n-1}s}$ durch p^n teilbar;
lässt sich $\sqrt{5}$ in der Arithmetik modulo p nicht ziehen, so sind die Zahlen der Form $a_{(p+1)p^{n-1}s}$ durch p^n teilbar.

Für $p = 2$ und $p = 5$ lassen sich die Indizes der Zahlen, die durch eine Potenz von p teilbar sind, unmittelbar finden. Wir schreiben die Fibonaccische Folge

$$0, 1, 1, 2, 3, 5, ...$$

auf und sehen, dass a_3 durch 2 und a_5 durch 5 teilbar ist. Daher ist $a_{3\cdot 2^{n-1}s}$ durch 2^n teilbar und $a_{5\cdot 5^{n-1}s} = a_{5^n\cdot s}$ durch 5^n.

Wir sind nun in der Lage, für jede Zahl m in der Fibonaccischen Folge Zahlen zu finden, die durch m teilbar sind. Als Beispiel wollen wir die Indizes derjenigen Zahlen suchen, die durch 10000 teilbar sind.
Wir zerlegen 10000 in die Faktoren 2^4 und 5^4. Durch 2^4 sind die Zahlen mit den Indizes $3 \cdot 2^{4-1}s = 24s$ teilbar, d.h. die Zahlen, deren Index durch 24 teilbar ist; durch 5^4 sind die Zahlen mit den Indizes $5^4t = 625t$ teilbar, d.h. alle Zahlen, deren Index durch 625 teilbar ist. Die Zahlen mit einem durch 24 und 625 teilbaren Index sind durch 10000 teilbar.

Die Indizes dieser Zahlen haben die Form

$$24 \cdot 625r = 15000r$$

Wir weisen darauf hin, dass unser Verfahren im allgemeinen nicht die Indizes aller Zahlen der Fibonaccischen Folge liefert, die durch ein gegebenes m teilbar sind. So ist

in unserem Beispiel die Zahl mit dem Index 12 ($a_12 = 144$) durch 2^4 teilbar. Daher sind durch 2^4 alle Zahlen mit den Indizes $12s$ teilbar und durch 10000 alle Zahlen mit den Indizes

$$12 \cdot 625r = 7500r$$

Betrachten wir noch ein Beispiel. Es soll bestimmt werden, welche Zahlen der Fibonaccischen Folge durch 55566 teilbar sind.
Wir zerlegen in Faktoren: $55566 = 2 \cdot 3^4 \cdot 7^3$. Durch 2 sind alle Zahlen mit der Nummer $3s$ teilbar. In der Arithmetik modulo 3 bedeutet $\sqrt{5}$ die Zahl $\sqrt{2}$ (2 ist der Rest bei der Division von 5 durch 3), und $\sqrt{5}$ lässt sich in der Arithmetik modulo 3 nicht ziehen. Folglich sind die Zahlen mit den Indizes $(3+1)3^{4-1}t = 108t$ durch 3^4 teilbar.

In der Arithmetik modulo 7 lässt sich $\sqrt{5}$ ebenfalls nicht ziehen, deshalb sind durch 7^3 die Zahlen mit den Indizes

$$(7+1)7^{3-1}q = 392q$$

teilbar.
Durch 55566 sind die Zahlen mit den Indizes $10584r$ teilbar, dabei ist 10584 das kleinste gemeinsame Vielfache der Zahlen 3, 108 und 392.

Dem Leser, der sich besonders für die Zahlen der Fibonaccischen Folge interessiert, sei auf die Arbeit von W. Ness, Die Fibonaccischen Zahlen, in "Der Mathematikunterricht" 11 (1965), Heft 5, S. 60-82, verwiesen.

5 Die Gleichung $x^2 - 5y^2 = 1$

Wir stellen uns die Aufgabe: Man suche alle ganzzahligen Lösungen der Gleichung[31]

$$x^2 - 5y^2 = 1 \tag{1}$$

d.h. alle Paare von ganzen Zahlen a, b, für die

$$a^2 - 5b^2 = 1$$

gilt.
Jedem Paar ganzer Zahlen a, b ordnen wir die irrationale Zahl $a + b\sqrt{5}$ zu, die wir eine Lösung der Gleichung (1) nennen wollen.
Später zeigen wir, dass man die Gesamtheit der Lösungen der Gleichung (1) aus der Formel

$$x + y\sqrt{5} = \pm(9 + 4\sqrt{5})^n$$

erhält, wobei n alle ganzen (nicht notwendig positiven) Zahlen durchläuft.
Wir empfehlen dem Leser, vor dem Weiterlesen zu versuchen, dies selbständig zu beweisen.

[31] Die Gleichung (1) ist ein Spezialfall der Gleichung $x^2 - Ay^2 = 1$, worin A eine positive ganze Zahl ist mit der Eigenschaft, dass $\sqrt{A}$ irrational ist. Die Aufgaben, die wir zur Gleichung (1) stellen, lassen sich auch für die allgemeine Gleichung lösen.

Wir weisen zuerst einige Eigenschaften der ganzen Zahlen der Form $p + q\sqrt{5}$ nach.[32]

119. Man beweise, dass aus $a + b\sqrt{5} = c + d\sqrt{5}$ folgt, dass $a = c$ und $b = d$ ist

120. Man beweise, dass sich das Produkt $(a + b\sqrt{5})(c + d\sqrt{5})$ wieder in der Form $p + q\sqrt{5}$ darstellen lässt. Man überzeuge sich davon, dass für $a \geq 0$, $b \geq 0$, $c \geq 0$ und $d \geq 0$ auch $p \geq 0$ und $q \geq 0$ ist.

121. Aus

$$m + n\sqrt{5} = (a + b\sqrt{5})(c + d\sqrt{5}) \qquad \text{folgt} \qquad m - n\sqrt{5} = (a - b\sqrt{5})(c - d\sqrt{5})$$

Wir wollen nun die Lösungen der Gleichung (1) untersuchen.

122. Es sei $a + b\sqrt{5}$ eine Lösung der Gleichung (1). Man beweise, dass
a) $a - b\sqrt{5}$ ebenfalls eine Lösung der Gleichung (1) ist;
b) $\frac{1}{a+b\sqrt{5}} = a - b\sqrt{5}$ gilt.

123. Es seien $a + b\sqrt{5}$ und $c + d\sqrt{5}$ Lösungen der Gleichung (1). Man beweise, dass
a) ihr Produkt $m + n\sqrt{5} = (a + b\sqrt{5})(c + d\sqrt{5})$ eine Lösung der Gleichung (1) ist;
b) ihr Quotient $\frac{a+b\sqrt{5}}{c+d\sqrt{5}}$ sich in der Form $p + q\sqrt{5}$ darstellen lässt und ebenfalls Lösung der Gleichung (1) ist.

124. Man weise nach, dass $9 + 4\sqrt{5}$ eine Lösung der Gleichung (1) ist, und beweise, dass die Gleichung (1) unendlich viele verschiedene ganzzahlige Lösungen hat.

125. Es seien $a + b\sqrt{5}$ und $c + d\sqrt{5}$ Lösungen der Gleichung (1), wobei $a \geq 0$, $b \geq 0$, $c \geq 0$ und $d \geq 0$ ist. Man beweise: Aus

$$a + b\sqrt{5} < c + d\sqrt{5}$$

folgt $a < c$ und $b < d$.

126. Es sei $a + b\sqrt{5}$ eine Lösung der Gleichung (1). Man beweise:
a) Aus $0 < a + b\sqrt{5}$ folgt $a \geq 0$,
b) Aus $1 < a + b\sqrt{5}$ folgt $a \geq 0$ und $b \geq 0$.

127. Man zeige, dass keine ganzzahlige Lösung der Gleichung (1) existiert, die der Ungleichung

$$1 < a + b\sqrt{5} < 9 + 4\sqrt{5}$$

genügt.

128. Man beweise, dass sich alle ganzzahligen Lösungen $p + q\sqrt{5}$ der Gleichung (1), bei denen $p \geq 0$ und $q \geq 0$ ist, aus der Formel

$$p + q\sqrt{5} = (9 + 4\sqrt{5})^n$$

ergeben, wobei n alle möglichen ganzzahligen nichtnegativen Werte durchläuft.

[32] In Kapitel 5 bedeuten alle Buchstaben, insbesondere p und q, ganze Zahlen.

129. Man beweise, dass man alle ganzzahligen Lösungen der Gleichung $x^2 - 5y^2 = 1$ aus der Formel

$$x + y\sqrt{5} = \pm(9 + 4\sqrt{5})^n$$

erhält, wobei n alle möglichen ganzzahligen Werte

$$0, \pm 1, \pm 2, \pm 3, \pm 4, ...$$

annimmt.

6 Ergänzung

Die Arithmetik der p-adischen Zahlen hat ebenso wie die Arithmetik modulo p große Ähnlichkeit mit der Arithmetik der rationalen (oder reellen) Zahlen.
Diese Ähnlichkeit besteht darin, dass in diesen Arithmetiken vier Rechenoperationen - Addition, Subtraktion, Multiplikation und Division - definiert sind, welche stets ausführbar sind und allen Gesetzen der gewöhnlichen Algebra genügen. Infolgedessen lässt sich die gewöhnliche Algebra in einer Arithmetik modulo p und in der Arithmetik der p-adischen Zahlen ebenso gut anwenden wie in der gewöhnlichen Arithmetik.

Eine beliebige Identität in Buchstaben, die nur die Operationen Addition, Subtraktion, Multiplikation und. Division enthält, ergibt beim Einsetzen von Zahlen aus einer Arithmetik modulo p eine richtige Gleichung modulo p und beim Einsetzen von p-adischen Zahlen eine Gleichung, die in der p-adischen Arithmetik gilt, ebenso wie man eine gültige Gleichung der gewöhnlichen Arithmetik erhält, wenn man reelle Zahlen einsetzt.

In der modernen Algebra heißt jedes System von Elementen, in dem die Operationen der Addition, Subtraktion, Multiplikation und Division definiert sind und allen Gesetzen der gewöhnlichen Algebra genügen, ein Körper.
Demnach sind die Systeme der p-adischen Zahlen sowie die Arithmetiken modulo p Körper. Ebenso sind die Menge aller rationalen Zahlen sowie die Menge aller reellen Zahlen Körper.

Die ganzen Zahlen hingegen bilden keinen Körper: Addition, Subtraktion und Multiplikation führen nicht aus dem Bereich der ganzen Zahlen heraus, die Division ist jedoch nicht immer ausführbar.

Systeme von Elementen, in denen die Operationen der Addition, Subtraktion und Multiplikation definiert sind und alle Gesetze der gewöhnlichen Algebra erfüllen, heißen (kommutative) Ringe. Als Beispiele für kommutative Ringe können angeführt werden: die Menge aller ganzen Zahlen, die Restklassen modulo m bei beliebigem m, die Arithmetiken der m-adischen Zahlen, die Menge aller Zahlen der Form $a+b\sqrt{5}$ mit ganzzahligem a und b, die Menge aller Polynome mit rationalen (oder reellen) Koeffizienten, die Menge aller Polynome mit Koeffizienten aus einer Arithmetik modulo p und allgemein die Menge aller Polynome mit Koeffizienten aus einem beliebigen Körper.
Offenbar ist jeder Körper ein kommutativer Ring.

Es zeigt sich, dass alle Gesetze der Algebra auf eine geringe Zahl von Grundgesetzen reduziert werden können. Im einzelnen werden diese Grundgesetze gewöhnlich wie folgt gefasst:

1. $a + b = b + a$ (Kommutativität oder Vertauschbarkeit der Addition);

2. $(a + b) + c = a + (b + c)$ (Assoziativität der Addition);

3. zu jedem a und b existiert die Differenz, d.h., es existiert ein x derart, dass $a+x = b$ (mit anderen Worten, die Subtraktion ist stets ausführbar);

4. $ab = ba$ (Kommutativität oder Vertauschbarkeit der Multiplikation);

5. $(ab)c = a(bc)$ (Assoziativität der Multiplikation);

6. $a(b + c) = ab + ac$ (Distributivität der Multiplikation bezüglich der Addition);

7. zu jedem b und jedem $a \neq 0$ existiert der Quotient, d.h., es existiert ein x derart, dass $ax = b$ gilt (Möglichkeit der Division).

Demnach kann ein Körper als ein System von Elementen definiert werden, in welchem die Operationen der Addition und Multiplikation definiert sind und die Forderungen 1. bis 7. erfüllen. Analog kann ein kommutativer Ring als ein System von Elementen definiert werden, das die Forderungen 1. bis 6. erfüllt.[33]

In diesem Abschnitt begegnete uns noch eine andere Kategorie algebraischer Systeme, die als Gruppen bezeichnet werden. Zwischen den Elementen einer Gruppe besteht eine Operation, die man Komposition nennt. Die Komposition der Elemente a und b wollen wir durch $a * b$ bezeichnen. Diese Operation genügt folgenden Gesetzen:

I. Für jedes Elementetripel gilt $(a * b) * c = a * (b * c)$.

II. Es existiert ein Einselement, d.h., es existiert ein Element e derart, dass $e * a = a$ für jedes a gilt.

III. Zu jedem Element a existiert ein Inverses, d.h., es existiert ein Element a^{-1} mit der Eigenschaft $a^{-1} * a = c$.

Das Produkt von Lösungen der Gleichung $x^2 - 5y^2 = 1$ war wieder eine Lösung dieser Gleichung. Nehmen wir dieses Produkt als Komposition von Lösungen an, so bilden die Lösungen eine Gruppe (da auch die anderen Forderungen erfüllt sind). Eine Gruppe bildet auch die Menge der gebrochenen linearen Funktionen mit Koeffizienten aus einem beliebigen Körper, wenn die Komposition wie folgt definiert wird:[34]

$$f(x) * g(x) = f(g(x))$$

Schließlich bilden alle von Null verschiedenen Elemente eines beliebigen Körpers eine Gruppe (als Komposition ist die Multiplikation zu nehmen), desgleichen alle Elemente eines beliebigen Ringes (als Komposition nehme man die Addition). Wir überlassen es dem Leser nachzuprüfen, dass alle diese Mengen tatsächlich Gruppen sind (man muss die Gültigkeit der Gesetze I, II, III nachweisen).

Die Begriffe Gruppe, Ring und Körper sind grundlegende Begriffe der modernen Algebra und spielen eine hervorragende Rolle in der gesamten Mathematik.

Für das Studium der Theorie der Körper können folgende Bücher empfohlen werden:

B.L. van der Waerden, Algebra (2 Bde.), Berlin 1971 bzw. 1967 (8. bzw. 5. Aufl.).

R. Kochendörffer, Einführung in die Algebra, Berlin 1966 (4. Aufl.).

[33] Systeme, die die Grundgesetze 1. bis 3. und 5. bis 6. erfüllen (die das Grundgesetz 4. nicht zu erfüllen brauchen) und für die weiterhin $(b + c)a = ba + ca$ gilt, heißen einfach Ringe (auch Schiefringe).

[34] In diesem Beispiel ist die Komposition zweier Elemente von der Reihenfolge abhängig, d.h., im allgemeinen ist $f(g(x))$ nicht gleich $g(f(x))$ (siehe Aufgabe 95).

Die Aufgaben, die wir in diesem Buch gestellt haben, liegen auf der Grenze zwischen Algebra und Zahlentheorie; man bezeichnet daher dieses Gebiet als algebraische Zahlentheorie.

Für die Entwicklung dieser Theorie waren die Arbeiten folgender Autoren grundlegend:

Carl Friedrich Gauß (1777-1855), Evariste Galois (1811-1832), Ernst Kummer (1810-1893), Leopold Kronecker (1823-1891), Igor Iwanowitsch Solotarjow (1847-1878), Richard Dedekind (1831 bis 1916), David Hilbert (1862-1943).

Die Theorie der p-adischen Zahlen, die wir in Kapitel 2 behandelt haben, wurde von Ernst Kummer und Kurt Hensel entwickelt. Von den Arbeiten zur algebraischen Zahlentheorie, die im Laufe der letzten Jahrzehnte erschienen sind, erwähnen wir die Arbeiten von N.G. Tschebortarjow, H. Hasse, E. Hecke, E. Landau, C.L. Siegel und I.R. Schafarewitsch.

Aus der populärwissenschaftlichen Literatur über algebraische Zahlentheorie seien genannt:

G. Rademacher und O. Toeplitz, „Zahlen und Figuren, Proben mathematischen Denkens für Liebhaber der Mathematik“, Springer, Berlin 1933.

7 Lösungen

1. Wir haben

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

Das Produkt einer beliebigen Zahl mit der Zahl 0 ist wie in der gewöhnlichen Arithmetik stets gleich Null. Es kann jedoch im Unterschied zur gewöhnlichen Arithmetik auch gleich Null sein, wenn jeder der Faktoren von Null verschieden ist. Die Zahlen 0, 2, 4, 6, 8, 5, die beim Multiplizieren mit einer von Null verschiedenen Zahl Null ergeben, heißen Nullteiler.

2. Wir erhalten

$$1 = 1 \cdot 1 = 3 \cdot 7 = 9 \cdot 9$$

Wir weisen darauf hin, dass in diesen Gleichungen keine Zahl steht, die Nullteiler ist, alle übrigen Zahlen jedoch kommen ausnahmslos vor.

3. Zur Lösung der Aufgaben genügt die Berechnung der Ausdrücke 6^{811}, 2^{1000} und 3^{999} modulo 10. In der Arithmetik modulo 10 gilt die Identität $6^2 = 6$. Wird diese Identität der Reihe nach mit $6, 6^2, 6^3, ...$ multipliziert, so erhält man

$$6^3 = 6^2, \quad 6^4 = 6^3, \quad 6^5 = 6^4, ...$$

Hieraus folgt $6^n = 6$ für beliebig vorgegebenes n. Insbesondere gilt $6^{811} = 6$.
Zur Berechnung von 2^{1000} bemerken wir, dass $2^4 = 6$ ist; folglich gilt $2^{1000} = 2^{4 \cdot 500} = 6^{250} = 6$.
Schließlich besteht auf Grund der Identität $3^4 = 1$ die Gleichung

$$3^{999} = 3^{4 \cdot 249 + 3} = (3^4)^{249} \cdot 3^3 = 3^3 = 7$$

4.

Additionstafel

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Multiplikationstafel

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Die Zerlegungen der Null und der Eins in Faktoren haben die Form

$$0 = 0 \cdot 0 = 1 \cdot 0 = 2 \cdot 0 = 3 \cdot 0 = 4 \cdot 0 = 5 \cdot 0 = 6 \cdot 0,$$
$$1 = 1 \cdot 1 = 2 \cdot 4 = 3 \cdot 5 = 6 \cdot 6$$

Wir stellen fest, dass modulo 7 das Produkt zweier Zahlen nur dann gleich Null ist, wenn einer der beiden Faktoren gleich Null ist. Hierin ist die Arithmetik modulo 7 der

gewöhnlichen Arithmetik ähnlich und von der Arithmetik modulo 10 verschieden.

Wir stellen nun die Multiplikationstafel der Arithmetik modulo 7 der Multiplikationstafel der Arithmetik modulo 10 gegenüber. Zwischen diesen Tafeln besteht folgender wesentlicher Unterschied:

In jeder Zeile der Tafel modulo 7 (außer derjenigen, die zur Null gehört) stehen alle Zahlen modulo 7, und zwar jede einmal; hingegen fehlen in der Multiplikationstafel modulo 10 in einzelnen Zeilen einige Restklassen, während andere wiederholt vorkommen. Solche Zeilen mit Wiederholungen sind, mit Ausnahme der Zeile 0, die Zeilen 2, 4, 5, 6, 8, d.h. diejenigen, die den Nullteilern entsprechen (siehe Lösung der Aufgabe 1).

Dass in der Multiplikationstafel modulo 7 Wiederholungen fehlen, hängt damit zusammen, dass es modulo 7 keine von 0 verschiedenen Nullteiler gibt.

5. Wir berechnen 3^{100} in der Arithmetik modulo 7: $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Hieraus folgt

$$3^{100} = 3^{6\cdot 16+4} = (3^6)^{16} \cdot 3^4 = 3^4 = 4$$

6. Wir stellen die Tafeln für die Arithmetik modulo 2 und modulo 4 auf:

modulo 2

Additionstafel

	0	1
0	0	1
1	1	0

Multiplikationstafel

	0	1
0	0	0
1	0	1

modulo 4

Additionstafel

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Multiplikationstafel

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Die Multiplikationstafeln der Arithmetik modulo 2 und der Arithmetik modulo 3 sind vom gleichen Typ wie die Tafel modulo 7; denn mit Ausnahme der Zeile 0 gibt es in ihnen keine Zeile mit Wiederholungen. Dagegen enthalten die Multiplikationstafeln modulo 4 und modulo 9 genau wie die modulo 10 außer der Zeile Null noch weitere Zeilen mit Wiederholungen.

7. Lösung: $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 10, 2^{10} = 3^{10} = ... = 10^{10} = 1$

8. Lösung: $1; 1; 1; 3$.

9. Es ist zu beweisen, dass in der Arithmetik modulo 1001

$$1^3 + 2^3 + 3^3 + ... + 500^3 + 501^3 + ... + 998^3 + 999^3 + 1000^3 = 0 \qquad (1)$$

gilt. Nun ist aber in der Arithmetik modulo 1001

$$\begin{aligned} 1000 &= -1, & 1000^3 &= (-1)^3 = -1^3, \\ 999 &= -2, & 999^3 &= (-2)^3 = -2^3, \\ 998 &= -3, & 998^3 &= (-3)^3 = -3^3, \\ &... \\ 501 &= -500, & 501^3 &= (-500)^3 = -500^3 \end{aligned}$$

Daher heben sich die entsprechenden Zahlen der Summe (1) gegenseitig auf.

10. a) Siehe Lösung der Aufgabe 9.
b) Der Ausdruck $1^k + 2^k + ... + (m-1)^k$ ist modulo m gemäß Aufgabe a) gleich Null. Folglich ist er in der gewöhnlichen Arithmetik durch m teilbar.

11. Als Beispiele stellen wir das Schema der Multiplikation mit 3 in der Arithmetik modulo 7 (Abb. 3.12), das Schema der Multiplikation mit 5 in der Arithmetik modulo 10 (Abb. B. 13) und das Schema der Multiplikation mit 3 in der Arithmetik modulo 9 (Abb. 13.14) auf.
Das erste dieser Schemata zerfällt in Zyklen, was man von den beiden anderen Schemata nicht sagen kann.

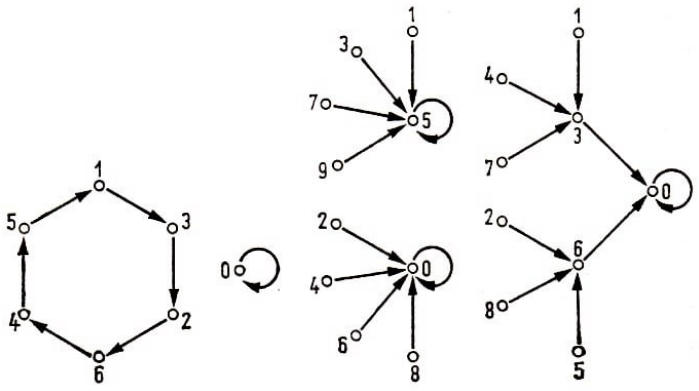


Abb. B.12,13,14

12. Um das Produkt der Zahlen a und b modulo p zu finden, genügt es, ihr Produkt im gewöhnlichen Sinne zu bilden und dessen Rest bei der Division durch p zu benutzen.
Daher ist ein Produkt in einer Arithmetik modulo p dann und nur dann gleich Null, wenn das gewöhnliche Produkt durch p teilbar ist. Jedoch ist, wie aus der gewöhnlichen Arithmetik bekannt ist, ein Produkt nur dann durch eine Primzahl p teilbar, wenn einer der Faktoren durch p teilbar ist.
Folglich ist a oder b durch p teilbar; da aber a und b unter den Zahlen $0, 1, 2, ..., p-1$ enthalten sind, ist $a = 0$ oder $b = 0$.

Anmerkung. Folgende Tatsache ist leicht zu beweisen: Folgt in einer Arithmetik modulo m aus a$b = 0$, dass $a = 0$ oder $b = 0$ ist, so ist m eine Primzahl. Hieraus und aus Aufgabe 12 geht hervor, dass Wir eine Arithmetik modulo p als Arithmetik modulo m definieren können, die keine von Null verschiedenen Nullteiler enthält.

13. a) Falls zur Zahl x zwei Pfeile weisen würden, etwa von den Zahlen y und z, so würde dies bedeuten, dass $ay = x$ und $az = x$ ist. Subtrahieren wir die zweite dieser Gleichungen von der ersten, so erhalten wir $a(y - z) = 0$, was jedoch gemäß Aufgabe 12 unmöglich ist, weil $a \neq 0$ und $y \neq z$ vorausgesetzt war.

b) Von jeder Zahl geht genau ein Pfeil aus. Demgemäß ist die Anzahl der Pfeile in dem Schema die gleiche wie die Anzahl der Punkte des Schemas, nämlich gleich p. Jeder Pfeil führt zu irgendeiner Zahl. Würde zu irgendeiner Zahl überhaupt kein Pfeil weisen, so müssten zu irgendeiner anderen Zahl zwei Pfeile weisen, was jedoch nach Aufgabe 3) unmöglich ist.

Zur Verdeutlichung der durchgeführten Überlegung bemerken wir, dass sie folgender Überlegung völlig analog ist. Wir nehmen an, in einer Klasse mit 30 Schülern seien 30 Hefte ausgegeben worden; ist bekannt, dass keiner der Schüler mehr als ein Heft besitzt, so kann man daraus schließen, dass jeder Schüler ein Heft besitzt (Dirichletscher Schubfachschluss; d. Red).

14. Wir betrachten das Schema der Multiplikation mit a. Gemäß Aufgabe 13 b) weist zur Zahl b ein Pfeil von einer Zahl x. Das heißt aber gerade, dass $ax = b$ ist.

15. a) Es sei b eine beliebige Zahl aus einer Arithmetik modulo p. Wir zeigen, dass b in einem Zyklus enthalten ist.
Wir bewegen uns von b aus auf unserem Schema, indem wir in Pfeilrichtung von Zahl zu Zahl gehen. Nach etlichen Schritten (die Anzahl der Schritte kann unter Umständen gleich 1 sein, aber niemals die Zahl p überschreiten) erreichen wir zum ersten Male einen Punkt, in dem wir uns bereits früher einmal befanden.

Dieser Punkt kann nur der Punkt b sein, denn sonst hätte unser Weg die in Abb. B.15 dargestellte Form, d.h., zu einer bestimmten Zahl würden zwei Pfeile führen, was jedoch auf Grund von Aufgabe 13 a) unmöglich ist.

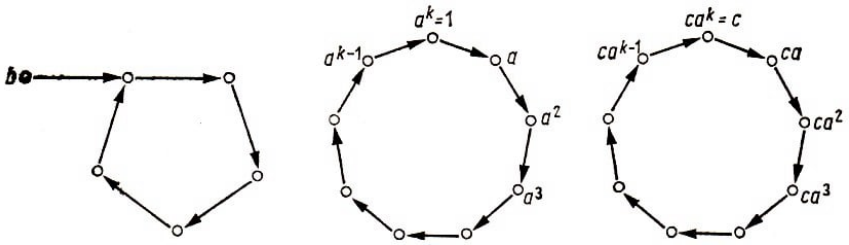


Abb. B.15,16,17

b) Wir betrachten den Zyklus, der die Zahl 1 enthält. Er habe das in Abb. 3.16 dargestellte Aussehen. Diesen Zyklus multiplizieren wir mit einer gewissen Zahl $c \neq 0$.
Wir erhalten einen neuen Zyklus unseres Schemas (Abb. B.17), der die gleiche Länge wie der ursprüngliche Zyklus hat. Es ist klar, dass jeder Zyklus C des Schemas, mit Ausnahme des Nullzyklus, auf folgender Art erhalten werden kann. Es genügt, den Einheitszyklus mit einer Zahl c aus C zu multiplizieren. Folglich haben alle von Null verschiedenen Zyklen die gleiche Länge.

Wir bezeichnen die Länge eines von Null verschiedenen Zyklus mit k und die Anzahl solcher Zyklen mit s. Dann gilt $ks = p - 1$. Andererseits war $a^k = 1$ (Abb. B.16). Erheben wir diese Gleichung in die s-te Potenz, so erhalten wir $a^{p-1} = 1$.

16. Das folgt daraus, dass in einer Arithmetik modulo p die Beziehung $a^{p1} - 1 = 0$ (siehe Aufgabe 15) gilt.

17. Die Tabellen der Kehrwerte sind in der Arithmetik modulo 7

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

in der Arithmetik modulo 11

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

in der Arithmetik modulo 13

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

Wir nehmen an, x sei gleich seinem Kehrwert, d.h. $x = \frac{1}{x}$. Dann ist $x^2 = 1$, woraus $(x-1)(x+1) = 0$ folgt. Gemäß Aufgabe 12 folgt hieraus $x - 1 = 0$ oder $x + 1 = 0$, d.h., es gilt $x = 1$ oder $x = -1$.

18. a) In dem Produkt $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ kürzt sich jede Zahl, außer 1 und $p - 1$, gegen ihren Kehrwert (siehe Aufgabe 17). Daher gilt

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

b) Folgt aus Aufgabe a).

19. Wir nehmen das Gegenteil an, es sei m keine Primzahl. Dann ist m durch irgendeine Zahl d teilbar, wobei $1 < d \leq m-1$. Daher ist $(m-1)!$ durch d teilbar, und $(m-1)!+1$, das ja durch m teilbar ist, ist ebenfalls durch d teilbar. Demnach muss jedoch auch die Differenz

$$[(m-1)! + 1] - (m-1)! = 1$$

durch d teilbar sein, was aber im Widerspruch zur Voraussetzung $d > 1$ steht.

20. Es ist zu zeigen, dass die Summe

$$S = 0^k + 1^k + 2^k + ... + (p-1)^k \tag{1}$$

gleich 0 oder gleich -1 ist.

Wir betrachten zuerst den Fall, dass für jede Zahl a ($a \neq 0$) aus einer Arithmetik modulo p die Beziehung $a^k = 1$ gilt.[35] Dann ist

$$S = 0^k + 1^k + 2^k + ... + (p-1)^k = 0 + \underbrace{1 + 1 + ... + 1}_{(p-1)-\text{mal}} = p - 1 = -1$$

Es gelte nun $a^k = 1$ nicht für alle von Null verschiedenen Zahlen a, d.h., es existiere eine Zahl $b \neq 0$ derart, dass $b^k \neq 1$ ist. Wir multiplizieren (I) mit b^k und erhalten

$$Sb^k = [0^k + 1^k + 2^k + ... + (p-1)^k]b^k = (0 \cdot b)^k + (1 \cdot b)^k + (2 \cdot b)^k + ... + [(p-1) \cdot b]^k$$

Unter den Zahlen $0 \cdot b$, $1 \cdot b$, ..., $(p-1) \cdot b$ kommen alle Zahlen der Arithmetik modulo p vor (für jedes a gilt $\frac{a}{b} \cdot b = a$). Außerdem kommt jede Zahl a hierin nur einmal vor, da aus $a = xb$ die Beziehung $x = \frac{a}{b}$ folgt. Daher ist

$$(0 \cdot b)^k + (1 \cdot b)^k + (2 \cdot b)^k + ... + [(p-1) \cdot b]^k$$

[35] Man sieht leicht ein, dass dieser Fall gilt, wenn k durch $p-1$ teilbar ist. Dann kann man beweisen, dass es keine anderen Möglichkeiten gibt, d.h., wenn $a^k = 1$ für jedes a gilt, so ist k durch $p-1$ teilbar (siehe Aufgabe 34).

die Summe (1), nur mit anderer Reihenfolge der Summanden, also

$$Sb^k = S \qquad , \qquad S(b^k - 1) = 0$$

Da $b^k - 1 \neq 0$ ist, kann man beide Seiten dieser Gleichung durch diesen Faktor dividieren und erhält $S = 0$.

21. Die Schemata für das Quadrieren sind: für die Arithmetik modulo 7 siehe Abb. B.18, für die Arithmetik modulo 12 siehe Abb. B.19, und für die Arithmetik modulo 24 siehe Abb. B.20.

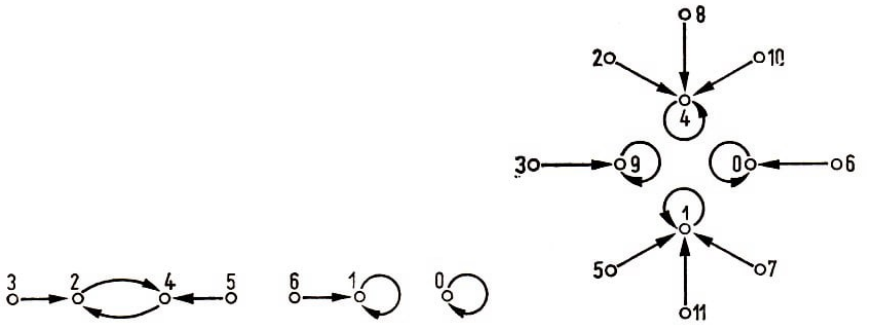


Abb. B.18,19

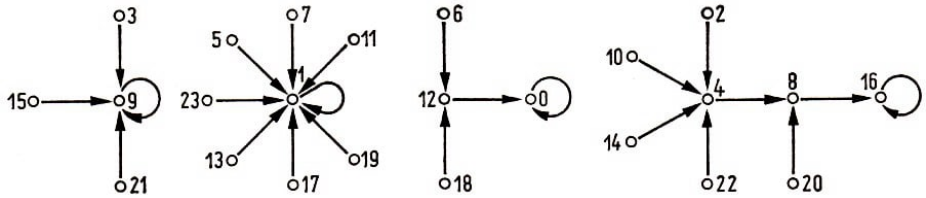


Abb. B.20

22. Wir nehmen an, die Gleichung

$$x^2 = a \tag{1}$$

werde durch irgendeine Zahl b der Arithmetik modulo p befriedigt, d.h., es gelte die Identität

$$b^2 = a \tag{2}$$

Subtrahiert man die Identität (2) von der Gleichung (1), so erhält man

$$x^2 - b^2 = 0 \qquad \text{also} \qquad (x - b)(x + b) = 0$$

Ist das Produkt zweier Zahlen aus einer Arithmetik modulo p gleich Null, so ist einer der beiden Faktoren gleich Null (Aufgabe 12). Daher gilt $x - b = 0$ oder $x + b = 0$, d.h. $x = b$ oder $x = -b$.
Wir beweisen, dass für $a \neq 0$ diese beiden Lösungen verschieden sind.

In der Tat, aus der Identität $b = -b$ folgte $b + b = 0$. Handelt es sich nicht um die Arithmetik modulo 2, so folgt hieraus $b = 0$ und somit auch $a = 0$.

23. Wir betrachten das Quadrier-Schema in der Arithmetik modulo p und diejenigen Zahlen, aus denen sich die Quadratwurzeln ziehen lassen, d.h. mit anderen Worten, jene Punkte, zu denen mindestens ein Pfeil führt.

Es sei k die Anzahl dieser Punkte. Dann führt laut Aufgabe 22 zu einem von ihnen, nämlich zum Punkt 0, ein Pfeil, zu den übrigen $(k-1)$ Punkten jedoch zwei Pfeile. Die Anzahl aller Pfeile in dem Schema ist demnach

$$2(k-1)+1$$

Andererseits geht von jedem Punkt genau ein Pfeil aus; im Schema gibt es jedoch p Punkte und folglich auch p Pfeile. Daher gilt

$$2(k-1)+1=p \qquad , \qquad k=\frac{p+1}{2}$$

24. a) Es sei $p=4k+1$. Auf Grund von Aufgabe 18 ist

$$1\cdot 2\cdot ...\cdot (p-1)=-1$$

Wir schreiben diese Gleichung in der Form

$$\begin{aligned}
-1 &= 1\cdot 2\cdot ...\cdot (p-1)\\
&= \left[1\cdot 2...\frac{p-3}{2}\cdot\frac{p-1}{2}\right]\left[\left(\frac{p-1}{2}-1\right)\left(\frac{p-1}{2}-2\right)...(p-2)(p-1)\right]\\
&= \left[1\cdot 2...\frac{p-3}{2}\cdot\frac{p-1}{2}\right]\left[\left(p-\frac{p-1}{2}\right)\left(p-\frac{p-3}{2}\right)...(p-2)(p-1)\right]\\
&= \left[1\cdot 2...\frac{p-3}{2}\cdot\frac{p-1}{2}\right]\left[(-1)(-2)...\left(-\frac{p-3}{2}\right)\left(-\frac{p-1}{2}\right)\right]\\
&= \left[1\cdot 2...\frac{p-3}{2}\cdot\frac{p-1}{2}\right]^2(-1)^{\frac{p-1}{2}}=\left[1\cdot 2...\frac{p-3}{2}\cdot\frac{p-1}{2}\right]^2(-1)^{2k}\\
&= \left[1\cdot 2...\frac{p-3}{2}\cdot\frac{p-1}{2}\right]^2(-1)^{\frac{p-1}{2}}
\end{aligned}$$

d.h., aus -1 lässt sich die Quadratwurzel ziehen.
Umgekehrt existiere nun $\sqrt{-1}$, d.h., es sei $x^2=-1$.
Wir erheben diese Gleichung in die $\frac{p-1}{2}$-te Potenz:

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

Auf Grund von Aufgabe 15 gilt

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

Hieraus folgt

$$(-1)^{\frac{p-1}{2}}=1 \qquad \text{und} \qquad \frac{p-1}{2}=2k, \quad p=4k+1$$

Demnach lässt sich die Quadratwurzel aus -1 nicht ziehen, wenn $p=4k+3$ ist.

b) Es sei a^2+1 durch p teilbar. In der Arithmetik modulo p lässt sich dieser Ausdruck

als $b^2+1=0$ schreiben (wobei b der Rest bei der Division von a durch p ist), d.h., $\sqrt{-1}$ lässt sich in der Arithmetik modulo p ziehen; hieraus folgt auf Grund der vorhergehenden Aufgabe $p=4k+1$.

Andererseits lässt sich, falls $p=4k+1$ ist, $\sqrt{-1}$ in der Arithmetik modulo p ziehen, d.h., es existiert ein a derart, dass $a^2=-1$ und $a^2+1=0$ ist. In der gewöhnlichen Arithmetik bedeutet das, dass a^2+1 durch p teilbar ist.

25. Die Formel wird genau wie in der gewöhnlichen Algebra hergeleitet.
Wir benutzen die Identität

$$ax^2+bx+c=a\left(x+\frac{b}{2a}\right)^2+\frac{4ac-b^2}{4a}$$

Gemäß dieser Identität ist die Gleichung

$$ax^2+bx+c=0 \tag{1}$$

äquivalent der Gleichung

$$a\left(x+\frac{b}{2a}\right)^2+\frac{4a-b^2}{4a}=0 \qquad \text{oder} \qquad \left(x+\frac{b}{2a}\right)^2=\frac{b^2-4a}{4a^2} \tag{2}$$

Aus der letzten Gleichung ist ersichtlich, dass sich die Quadratwurzel aus b^2-4ac ziehen lässt, wenn (1) eine Lösung hat. In diesem Fall kann man die Gleichung (2) in die Form

$$x+\frac{b}{2a}=\frac{\pm\sqrt{b^2-4ac}}{2a}$$

umschreiben, woraus

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

folgt.
Somit ist die Gleichung (1) nicht lösbar, wenn sich die Wurzel aus b^2-4ac nicht ziehen lässt, und sie hat zwei Lösungen, die sich nach Formel (3) berechnen, wenn $\sqrt{b^2-4ac}$ existiert.
Diese beiden Lösungen sind im Fall $b^2-4ac\neq 0$ voneinander verschieden und fallen für $b^2-4ac=0$ zusammen. In der Arithmetik modulo 2 verliert die Formel (3) ihren Sinn, da sie eine Division durch 2 enthält.

26. Wir berechnen für jede der gegebenen Gleichungen die Diskriminante $D=b^2-4ac$. Für die erste Gleichung erhalten wir $D=3$, für die zweite $D=0$ und für die dritte $D=2$.
Wir benutzen beispielsweise das Schema in Aufgabe 21 (Abb. B. 18) und stellen fest, dass sich $\sqrt{3}$ in der Arithmetik modulo 7 nicht ziehen lässt, jedoch lässt sich $\sqrt{2}$ ziehen und hat die Werte 3 und 4.
Folglich hat die erste Gleichung keine, die zweite genau eine und die dritte zwei Lösungen. Diese Lösungen finden wir nach Formel (3) aus Aufgabe 25: Für die zweite Gleichung ist $x=2$, für die dritte ist $x_1=3$ und $x_2=6$.

27. Sind α und β Wurzeln der Gleichung $x^2 + +cx + d = 0$, so gilt wie in der gewöhnlichen Algebra

$$x^2 + cx + d = (x - \alpha)(x - \beta)$$

(Um sich hiervon zu überzeugen, genügt es, α und β durch c und d mit Hilfe der Formeln zur Lösung quadratischer Gleichungen auszudrücken und die Klammern aufzulösen.)

Daher ist die Anzahl der reduzierten Gleichungen, die zwei verschiedene Wurzeln besitzen, gleich der Anzahl der Arten, auf welche zwei verschiedene Zahlen α und β aus der Gesamtheit aller p Zahlen der Arithmetik modulo p gewählt werden können, d.h. gleich $\frac{p(p-1)}{2}$. Falls die Gleichung $x^2 + cx + d = 0$ nur eine Wurzel hat, so gilt

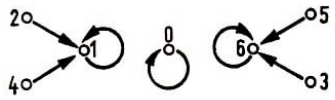
$$x^2 + cx + d = (x - \alpha)^2$$

Die Anzahl dieser Gleichungen ist gleich p. Alle anderen Gleichungen (ihre Anzahl ist gleich

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

haben keine Lösung.

28. Nachstehend sind die Schemata für die Kuben angegeben; und zwar für die Arithmetik modulo 7 in Abb. B.21, für die Arithmetik modulo 11 in Abb. B.22, für die Arithmetik modulo 13 in Abb. B.23 und für die Arithmetik modulo 17 in Abb. B.24.



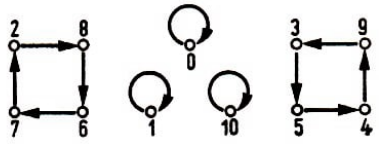
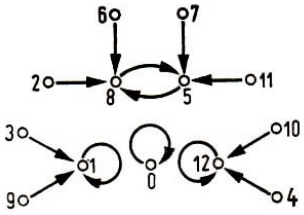


Abb. B.21,22



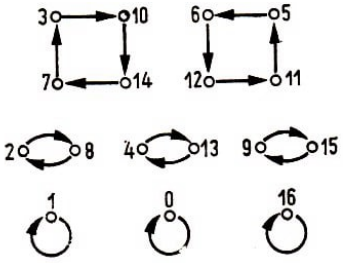


Abb. B.23,24

29. a) Es sei

$$b^3 = 1 \tag{1}$$

Gemäß Aufgabe 15 ist

$$b^{p-1} = 1 \tag{2}$$

Wegen $p = 3k + 2$ ist $p - 1 = 3k + 1$, und die Gleichung (2) erhält die Form

$$b_{3k+1} = 1 \tag{3}$$

Wird die Gleichung (1) in die k-te Potenz erhoben, so erhalten wir

$$b^{3k} = 1 \tag{4}$$

und durch Division von (3) durch (4) folgt

$$b = 1 \tag{5}$$

Damit ergibt sich (5) aus (1), was zu beweisen war.

b) Es sei $x^3 = a$ und $y^3 = a$. Durch Division der ersten dieser Gleichungen durch die zweite erhalten wir $\left(\frac{x}{y}\right)^3 = 1$, woraus gemäß Aufgabe a) $\frac{x}{y} = 1$ folgt, d.h. aber $x = y$.

c) Wir stellen folgende Tabelle auf:

$$\begin{array}{cccccc} 0, & 1, & 2, & 3, & ..., & p-1, \\ 0^3, & 1^3, & 2^3, & 3^3, & ..., & (p-1)^3 \end{array}$$

In der oberen Zeile stehen alle p Zahlen der Arithmetik modulo p, und unter einer jeden steht ihre dritte Potenz. Auf Grund des in Aufgabe b) Gezeigten besteht die untere Zeile aus p verschiedenen Zahlen, folglich sind in ihr Zahlen der Arithmetik modulo p enthalten.
Das heißt aber, dass sich aus jeder Zahl der Arithmetik modulo p die Kubikwurzel ziehen lässt.

30. Aus der Gleichung $(x-1)(x^2+x+1) = 0$ folgt, dass

$$x - 1 = 0 \qquad \text{oder} \qquad x^2 + x + 1 = 0$$

ist. Aus der ersten Gleichung erhalten wir $x_1 = 1$, und aus der zweiten

$$x_{2,3} = \frac{-1 \pm \sqrt{-3}}{2} \tag{1}$$

In der Arithmetik modulo 103 ist $-3 = 100$ und $\sqrt{-3} = \pm 10$. Setzen wir diese Werte für $\sqrt{-3}$ in Formel (1) ein, so ergibt sich $x_1 = 1$, $x_2 = 56$, $x_3 = 46$.

31. Jeder Wert der dritten Wurzel aus 1 erfüllt die Gleichung $x^3 - 1 = 0$, und falls er nicht gleich 1 ist, erfüllt er die quadratische Gleichung $x^2 + x + 1 = 0$.
Je nachdem, ob sich die Wurzel aus -3 in der Arithmetik modulo p ziehen lässt oder nicht, hat diese Gleichung zwei verschiedene Wurzeln, die aus (1) zu berechnen sind, oder sie hat gar keine Wurzel in der Arithmetik modulo p.

Ausnahmen sind die Arithmetik modulo 2 und die Arithmetik modulo 3. Die Formel (1) verliert in der Arithmetik modulo 2 ihren Sinn; in der Arithmetik modulo 3 ist $-3 = 0$; die Gleichung $x^2 + x + 1 = 0$ hat dann nur eine Wurzel, nämlich 1.

32. Es sei $p > 3$, und es existiere eine ganze Zahl a derart, dass $a^2 + 3$ durch p teilbar ist. Wenn der Rest bei der Division von a durch p gleich b ist, so ist in der Arithmetik modulo p

$$b^2 + 3 = 0 \qquad \text{oder} \qquad b^2 = -3$$

Das bedeutet, dass sich $\sqrt{-3}$ in der Arithmetik modulo p ziehen lässt. Auf Grund von Aufgabe 31 folgt hieraus, dass $\sqrt[3]{1}$ drei verschiedene Werte hat. Gemäß Aufgabe 29

kann p nicht die Form $3k+2$ haben und muss somit von der Form $3k+1$ sein.

33. Die Gleichung ersten Grades $ax+b=0$ hat nur die eine Lösung $x=-\frac{b}{a}$.
Unser Satz sei für Polynome n-ten Grades bewiesen. Wir zeigen, dass er dann auch für Polynome $(n+1)$-ten Grades Gültigkeit besitzt. Dazu nehmen wir das Gegenteil an. Das Polynom $(n+1)$-ten Grades

$$a_0x^{n+1}+a_1x^n+...+a_nx+a_{n+1}=0 \tag{1}$$

habe mindestens die $n+2$ Nullstellen $x_1,x_2,...,x_{n+1},x_{n+2}$. Wir bilden das Polynom

$$a_0(x-x_1)(x-x_2)...(x-x_{n+1}) \tag{2}$$

In diesem Polynom ist der Koeffizient von x^{n+1} gleich a_0, daher verschwinden in der Differenz

$$a_0x^{n+1}+a_1x^n+...+a_nx+a_{n+1}-a_0(x-x_1)(x-x_2)...(x-x_{n+1}) \tag{3}$$

die Glieder mit x^{n+1}, und (3) ist somit ein Polynom n-ten Grades. Es hat aber die $n+1$ Nullstellen $x_1,x_2,...,x_{n+1}$. Da nach Voraussetzung der Satz für Polynome n-ten Grades bewiesen sein sollte, sind alle Koeffizienten des Polynoms (3) gleich Null.
Diese sind jedoch die Differenzen entsprechender Koeffizienten der Polynome (1) und (2); daher sind alle Koeffizienten des Polynoms (1) gleich den Koeffizienten des Polynoms (2), d.h., die Polynome (1) und (2) sind identisch.
Dann muss aber (2) für $x=x_{n+2}$ verschwinden:

$$a_0(x_{n+2}-x_1)(x_{n+2}-x_2)...(x_{n+2}-x_{n+1})=0$$

was unmöglich ist wegen

$$a_0\neq 0,\quad x_{n+2}-x_1\neq 0,\quad ...,\quad x_{n+2}-x_{n+1}\neq 0$$

Der Satz ist für $n=1$ gültig; nach diesem Beweis gilt er auch für $n=1+1=2$, für $n=3$ und allgemein für jedes n.
Dieser Beweis ist sowohl in einer Arithmetik modulo p als auch in der gewöhnlichen Arithmetik gültig.

34. Der Rest bei der Division von k durch $p-1$ sei r:

$$k=q(p-1)+r \qquad , \qquad r<p-1$$

Dann gilt für alle x

$$x^{p-1}=1, \qquad x^{qp-1}=1, \qquad x^k=x^{q(p-1)+r}=1 \tag{1,2}$$

woraus man durch Division von (2) durch (1) für jedes x:

$$x^r=1$$

erhält. Wäre $r > 0$, so wären die Koeffizienten des Polynoms $x^r - 1$ nicht alle gleich Null. Jedoch ist die Anzahl seiner Nullstellen $p - 1 > r$ $(x = 1, 2, ..., p - 1)$, was der Aussage von Aufgabe 33 widerspricht.

35. Es ist

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

(Aufgabe 15), daher ist $a^{\frac{p-1}{2}} = \pm 1$. Wenn sich $\sqrt{a}$ ziehen lässt, d.h., wenn ein b existiert derart, dass $b^2 = a$ ist, so ist $a^{\frac{p-1}{2}} = b^{p-1} = 1$.
Somit ist a, wenn sich $\sqrt{a}$ ziehen lässt, Wurzel der Gleichung

$$x^{\frac{p-1}{2}} = 1 \tag{1}$$

Diese Gleichung hat nicht mehr als $\frac{p-1}{2}$ Wurzeln (Aufgabe 33). Andererseits gibt es genau $\frac{p-1}{2}$ von Null verschiedene Zahlen, aus denen sich die Quadratwurzel ziehen lässt, die sämtlich die Gleichung (1) erfüllen.
Daher wird die Gleichung (1) nur von denjenigen Zahlen erfüllt, aus denen sich die Quadratwurzel ziehen lässt. Für die übrigen Zahlen bleibt nur eine Möglichkeit:

$$a^{\frac{p-1}{2}} = -1$$

36. Der Beweis dieses Satzes ist in der Lösung der Aufgabe 33 enthalten. Der Vollständigkeit halber wiederholen wir hier unsere Überlegungen. Das Polynom

$$a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n - a_0(x - x_1)(x - x_2)...(x - x_n)$$

ist ein Polynom $(n-1)$-ten Grades mit n Nullstellen; aus diesem Grunde sind alle seine Koeffizienten gleich Null, und die Koeffizienten des Polynoms $a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$ stimmen mit den Koeffizienten des Polynoms $a_0(x - x_1)(x - x_2)...(x - x_n)$ überein.

37. Das Polynom $x^{p-1} - 1$ hat $p - 1$ Nullstellen: $1, 2, 3, ..., p - 1$. Gemäß Aufgabe 36 ist

$$x^{p-1} - 1 = (x - 1)(x - 2)...[x - (p - 1)]$$

Für $x = 0$ erhalten wir

$$-1 = (-1)(-2)...[-(p - 1)] = (-1)^{p-1} \cdot 1 \cdot 2...(p - 1) = 1 \cdot 2...(p - 1)$$

38. a)

372233	|	189^9	37233 : 189 = 197
- 1323	|	197	
3591			
-1701			
189			
-189			
0			

b) Wir kürzen Dividend und Divisor durch 8: $36408 : 328 = 4551 : 41$

4551	|	41^1	36408 : 328 = 111
- 41	|	111	
451			
-41			
41			
-41			
0			

c) Wir kürzen Dividend und Divisor durch 2: $851 : 74 = 425,5 : 37$

425,5	|	37^3	851 : 74 = 11,5
- 18,5	|	11,5	
407			
-37			
37			
-37			
0			

39. $1 : 3 = (6)7$, $1 : 7 = (285714)3$, $1 : 9 = (8)9$ (die Periode ist in Klammern angegeben).

40. a.) Wir bezeichnen mit x_n die n-te Zahl der Tabelle. Es ist $x_1 = 5$, $x_2 = 5^2$, $x_3 = x_2^2 = 5^{2^2}$, ..., $x_n = 5^{2^{n-1}}$. Wir zerlegen die Differenz $x_{n+1} - x_n$ in Faktoren:

$$\begin{aligned} x_{n+1} - x_n &= 5^{2^n} - 5^{2^{n-1}} = 5^{2^{n-1}}(5^{2^{n-1}} - 1) \\ &= 5^{2^{n-1}}(5^{2^{n-2}} + 1)(5^{2^{n-3}} + 1)(5^{2^{n-4}} + 1)...(5^2 + 1)(5 + 1)(5 - 1) \end{aligned}$$

Alle Faktoren, mit Ausnahme des ersten, sind gerade Zahlen, und da n derartige Faktoren vorkommen, ist das Produkt durch 2^n teilbar. Andererseits ist der erste Faktor durch 5^n teilbar, weil $2^{n-1} \geq n$ für $n \geq 1$ ist. Somit ist $x_{n+1} - x_n$ durch 10^n teilbar, oder, was dasselbe ist, die letzten n Ziffern der Zahlen x_{n+1} und x_n stimmen überein.

Wir nehmen nun den über der eingerahmten Hauptdiagonalen liegenden Teil der Tabelle heraus. Nach dem schon Bewiesenen stehen in jeder Spalte des übriggebliebenen Teiles der Tabelle gleiche Ziffern.
Hieraus ist ersichtlich, dass die letzten n Ziffern der Zahl x_n mit den letzten n Ziffern der Diagonalzahl $d = ...90625$ übereinstimmen oder, mit anderen Worten, $d - x_n = a_n 10^n$, wobei a_n eine unendlichstellige Zahl ist. Aus der letzten Gleichung folgt

$$d = x_n + a_n 10^n \qquad , \qquad d^2 = x_n^2 + 2x_n a_n 10^n + a_n^2 10^{2n}$$

Unter Benutzung der Gleichungen

$$x_n^2 = x_{n+1} \qquad \text{und} \qquad d = x_{n+1} + a_{n+1} 10^{n+1}$$

erhalten wir

$$d^2 - d = (x_n^2 + 2x_n a_n 10^n + a_n^2 10^{2n}) - (x_{n+1} + a_{n+1} 10^{n+1}) = 10^n(2x_n a_n + a_n^2 10^n - a_{n+1} 10)$$

Folglich stimmen die letzten n Ziffern der Zahlen d^2 und d überein. Da n eine beliebige natürliche Zahl ist, stimmen alle Ziffern von d^2 und d überein, d.h. $d^2 = d$.

b) Wir zeigen nun, dass $e^2 = e$ ist. In der Tat ist

$$e^2 = (1-d)^2 = 1 - 2d + d^2 = 1 - 2d + d = 1 - d = e$$

c) Schließlich ist

$$de = d(1-d) = d - d^2 = 0$$

Somit kann in der Arithmetik der unendlichstelligen Zahlen die Multiplikation zweier von Null verschiedener Zahlen Null ergeben. Diese Eigenschaft unterscheidet die Arithmetik der unendlichstelligen Zahlen von der gewöhnlichen Arithmetik und lässt sie der Arithmetik modulo 10 verwandt erscheinen.

41. Wir nehmen das Gegenteil an und betrachten das Produkt xde.
Aus der Gleichung $xd = 1$ folgt $xde = 1 \cdot e = e$. Aus der Gleichung $de = 0$ folgt $xde = x \cdot 0 = 0$. Wir erhalten einen Widerspruch, weil $e \neq 0$ ist.

42. Eine Zahl x, die ihrem Quadrat gleich ist, muss eine ganze Zahl sein. In der Tat, wenn x hinter dem Komma k Dezimalstellen hat, wobei die letzte davon nicht Null ist, so hat x^2 hinter dem Komma $2k$ Dezimalstellen, deren letzte wiederum nicht Null ist. Daher gilt für $x^2 = x$ die Gleichung $2k = k$, d h. $k = 0$.

Ferner muss eine Zahl x, die ihrem Quadrat gleich ist, auf eine der Ziffern 0, 1, 5 oder 6 enden; sonst würden x und x^2 auf verschiedene Ziffern enden. Es sei

$$x^2 = x \qquad \text{und} \qquad y = 1 - x$$

Dann ist $y^2 = y$, denn es gilt

$$y^2 = (1-x)a = 1 - 2x + x^2 = 1 - 2x + x = 1 - x = y$$

Endet hierbei x auf eine der Ziffern 0 oder 5, so endet y auf eine der Ziffern 1 oder 6, und umgekehrt. Daher genügt es, alle die Zahlen zu finden, die ihrem Quadrat gleich sind und auf eine der Ziffern 0 oder 5 enden.
Es seien a und b zwei verschiedene Zahlen, die beide entweder auf Null oder auf 5 enden. Dann endet die Summe $a + b$ auf Null. Wegen

$$a^2 - b^2 = (a-b)(a+b)$$

hat die Differenz $a^2 - b^2$ am Ende mehr Nullen als die Differenz $a - b$. Folglich ist $a^2 - b^2 \neq a - b$, das bedeutet aber, dass entweder $a^2 \neq a$ oder $b^2 \neq b$ ist.
Damit ist bewiesen, dass es höchstens eine Zahl gibt, die ihrem eigenen Quadrat gleich ist und mit einer Null endet, und auch höchstens eine, die mit der Ziffer 5 endet. Wir wissen, dass diese Zahlen 0 und $d = ...90625$ sind.

43. Es sei $a = ...a_3a_2a_1$. Die letzte Ziffer des Produktes wird durch das Produkt der letzten Ziffern der Faktoren bestimmt, daher ist a^{p-1} die letzte Ziffer der Zahl a_1^{p-1} (im Sinne der Arithmetik modulo p).

In einer Arithmetik modulo p ist jedoch $a^{p-1} = 1$ (siehe Aufgabe 15). Folglich ist Null die letzte Ziffer der Zahl $a^{p-1} - 1$.

44. Wir beweisen dies durch vollständige Induktion. Der Fall $k = 1$ ist in der vorhergehenden Aufgabe dargestellt. Der Satz sei für $k = l$ bewiesen. Wir beweisen ihn für $k = l + 1$. Dazu bezeichnen wir $a^{p^{l-1}(p-1)}$ mit y und erhalten

$$ap^l(p-1) - 1 = y^p - 1^p = (y-1)(y^{p-1} + y^{p-2} + ... + y + 1)$$

Da $y - 1$ nach Induktionsvoraussetzung auf l Nullen endet, genügt es zu beweisen, dass $y^{p-1} + y^{p-2} + ... + 1$ auf 0 endet. Die letzte Ziffer von y ist 1; daher sind auch die letzten Ziffern aller Zahlen $y^2, y^3, ..., y^{p-1}$ Einsen. Hieraus folgt, dass die letzte Ziffer der Zahl

$$y^{p-1} + y^{p-2} + ... + y + 1 = \underbrace{...1 + ...1 + ... + ...1 + ...1}_{p-\text{mal}}$$

eine Null ist.

Anmerkung. Wird das Resultat dieser Aufgabe auf endlichstellige Zahlen angewendet, so erhalten wir folgenden Satz aus der gewöhnlichen Arithmetik:
Ist eine ganze Zahl a durch eine Primzahl p nicht teilbar, so ist $a^{p^{k-1}(p-1)} - 1$ durch p^k teilbar. Dieser Satz lässt sich folgendermaßen verallgemeinern.

Eulerscher Satz. Sind a und m teilerfremd, so ist $a^{\varphi(m)} - 1$ durch m teilbar.

Hierbei ist $\varphi(m)$ die Anzahl der zu m teilerfremden Zahlen zwischen 1 und m. Zum Beispiel gilt $\varphi(10) = 4$ (die zu 10 teilerfremden Zahlen zwischen 1 und 10 sind die Zahlen 1, 3, 7, 9). Wir überlassen dem Leser den Beweis der Beziehungen

$$\varphi(p) = p - 1 \qquad , \qquad \varphi(p^k) = p^{k-1}(p-1)$$

Der Eulersche Satz gilt nicht nur für endlichstellige Zahlen, sondern auch für unendlichstellige.

45. Die allgemeine Form des n-ten Gliedes einer geometrischen Reihe ist $b_n = b_0 q^n$. Daher gilt

$$b_{n+p^{k+1}(p-1)} = b_0 q^{n+p^{k-1}(p-1)} = b_n q^{p^{k-1}(p-1)}$$

Aus Aufgabe 44 folgt aber, dass $000...001$ die letzten k Ziffern der Zahl $q^{p^{k-1}(p-1)}$ sind. Hieraus geht hervor, dass die letzten k Ziffern der Zahlen b_n und $b_n q^{p^{k-1}(p-1)} = b_{n+p^{k-1}(p-1)}$ übereinstimmen.

46. Dies wird genau wie Aufgabe 22 gelöst, wobei lediglich für den Ausdruck "Arithmetik modulo p" der Ausdruck "Arithmetik der p-adischen Zahlen" zu setzen ist.

47. Diese Aufgabe wird genau wie Aufgabe 25 gelöst, wobei nur für den Ausdruck "Arithmetik modulo p" der Ausdruck "Arithmetik der p-adischen Zahlen" zu setzen ist.

48. Hat eine Zahl hinter dem Komma k von Null verschiedene Ziffern, so hat ihr Quadrat hinter dem Komma $2k$ von Null verschiedene Ziffern.

49. Die letzte Ziffer von a sei a_1, und die letzte Ziffer von $b = \sqrt{a}$ sei b_1. Dann gilt $b_1^2 = a_1$ in der Arithmetik modulo p.

50. Es ist nämlich

$$\begin{array}{r} 201 \\ \cdot\ 201 \\ \hline 201 \\ 000 \\ 1102 \\ \hline 111101 \end{array}$$

Die letzten drei Ziffern der Zahlen 111 101 und ...112 101 stimmen überein.

51. Mit dem Buchstaben u'_n bezeichnen wir den Ausdruck $a_{n-1}u_0 + a_n u_1$.
Die Folge $u'_0, u'_1, ..., u'_n, ...$ ist eine Fibonaccische Folge. Denn es ist

$$\begin{aligned} u'_{n-2} + u'_{n-1} &= (a_{n-3}u_0 + a_{n-2}u_1) + (a_{n-2}u_0 + a_{n-1}u_1) \\ &= (a_{n-3} + a_{n-2})u_0 + (a_{n-2} + a_{n-1})u_1 = a_{n-1}u_0 + a_n u_1 = u'_n \end{aligned}$$

Wir bemerken ferner, dass

$$u'_0 = a_{-1}u_0 + a_0 u_1 = u_0 \qquad , \qquad u'_1 = a_0 u_0 + a_1 u_1 = u_1$$

ist und somit die Folgen $u_0, u_1, u_2, ..., u_n, ...$ und $u'_0, u'_1, u'_2, ..., u'_n, ...$ die ersten beiden Glieder gemeinsam haben. Da beide Folgen Fibonaccische Folgen sind, sind sie völlig identisch, d.h., es gilt für jedes n

$$u_n = u'_n = a_{n-1}u_0 + a_n u_1$$

52. Es genügt, die Formel aus Aufgabe 51 auf die Fibonaccische Folge

$$a_{m-1}, a_m, a_{m+1}, a_{m+2}, ..., a_{m+(n+1)}, ...$$

anzuwenden, in der $u_n = a_{m+(n-1)}$ ist.

53. Wenn man in der Formel der vorhergehenden Aufgabe $m = n$ setzt, erhält man

$$a_{2n-1} = a_{n-1}^2 + a_n^2$$

54. Es sei

$$u_{n-1}u_{n+1} - u_n^2 = d_n$$

Wir erhalten dann

$$\begin{aligned} d_{n+1} &= u_n u_{n+2} - u_{n+1}^2 = u_n(u_n + u_{n+1}) - u_{n+1}^2 = u_n^2 + u_n u_{n+1} - u_{n+1}^2 \\ &= u_n^2 - u_{n+1}(-u_n + u_{n+1}) = u_n^2 - u_{n-1}u_{n+1} = -d_n \end{aligned}$$

Hieraus folgt

$$d_n = -d_{n-1} = (-1)^2 d_{n-2} = (-1)^3 d_{n-3} = ... = (-1)^{n-1} d_1 = (-1)^{n-1}(u_0 u_2 - u_1^2) \tag{1}$$

Wegen $a_0a_2 - a_1^2 = -1$ ist $a_{n-1}a_{n+1} - a_n^2 = (-1)^n$.

55. Wir bemerken, dass

$$\begin{aligned} u_{n-1}u_{n-2} - u_nu_{n+1} &= u_{n-1}u_n + u_{n-1}u_{n+1} - u_nu_{n+1} \\ &= u_{n-1}u_{n+1} - u_n(u_{n+1} - u_{n-1}) \\ &= u_{n-1}u_{n+1} - u_n^2 = (-1)^{n-1}(u_0u_2 - u_1^2) \end{aligned} \tag{1}$$

ist; hieraus folgt

$$|u_{n-1}u_{n+2} - u_nu_{n+1}| = |u_0u_2 - u_1^2|$$

Für die Folge F^0 gilt

$$a_{n-1}a_{n+2} - a_na_{n+1} = (-1)^{n-1}(a_0a_2a_1^2) = (-1)^{n-1}(0 \cdot 1 - 1) = (-1)^n$$

56. Die Endziffern der Zahlen der Fibonaccischen Folge F^0 bilden selbst wieder eine Fibonaccische Folge in der Arithmetik modulo 10 (nämlich die Folge F_{10}^0).
Wir schreiben uns die Glieder dieser Reihe auf :

$0, 1, 1, 2, 3, 5, 8, 3, 1, 4, 5, 9, 4, 3, 7, 0, 7, 7, 4, 1, 5, 6, 1, 7, 8, 5, 3, 8, 1, 9, 0, 9, 9, 8, 7, 5, 2, 7,$
$9, 6, 5, 1, 6, 7, 3, 0, 3, 3, 6, 9, 5, 4, 9, 3, 2, 5, 7, 2, 9, 1, 0, 1, 1, 2, 3, 5, ...$

und bemerken, dass $c_{60} = 0$ und $c_{61} = 1$ ist. Folglich erhalten wir, wenn wir in der Folge die ersten 60 Glieder $(c_0, c_1, ..., c_{59})$ streichen, wieder eine Fibonaccische Folge, die mit den Zahlen 0 und 1 beginnt, d.h. wieder die Folge F_{10}^0.
Es ist also $c_{62} = c_2$, $c_{63} = c_3$, ..., $c_{60+k} = c_k$, d.h., die F_{10}^0 ist periodisch, und die Länge einer Periode ist 60.

57. Gegeben sei eine Fibonaccische Folge $v_0, v_1, v_2, ..., v_n, ...$ Wir beweisen, dass für ein gewisses r die Gleichungen $v_r = v_0$, $v_{r+1} = v_1$ gelten, wonach sich genau wie in der vorhergehenden Aufgabe für F_{10}^0 die Periodizität der Folge $v_0, v_1, ..., v_n, ...$ beweisen lässt (wobei die Länge der Periode gleich r ist).

Eine Arithmetik modulo m hat insgesamt m Elemente. Aus diesen können nicht mehr als m^2 verschiedene Paare zusammengestellt werden. Daher kommen unter den $m^2 + 1$ derartigen Paaren (v_0, v_1), (v_1, v_2), (v_2, v_3), ..., (v_{m^2}, v_{m^2+1}) zwei gleiche Paare vor.
Es seien dies das k-te und das l-te Paar $(k < l \leq m^2 + 1)$, d.h., es sei

$$v_k = v_l \qquad , \qquad v_{k-1} = v_{l-1} \tag{1,2}$$

Subtrahieren wir (2) von (1), so erhalten wir

$$v_{k-2} = v_{l-2} \tag{3}$$

Wird (3) von (2) subtrahiert, so finden wir

$$v_{k-3} = v_{l-3}$$

Setzen wir diese Subtraktion fort, so erhalten wir schließlich

$$v_1 = v_{l-k+1} \qquad , \qquad v_0 = v_{l-k}$$

und nach Einsetzen von $l - k = r$

$$v_1 = v_{r+1} \qquad , \qquad v_0 = v_r$$

Wegen $l \leq m^2 + 1$ und $k \geq 1$ ist $r \leq m^2$.

58. Bei der Division der Zahlen einer Folge F^0 durch m bilden die Reste die Folge F_M^0. Auf Grund von Aufgabe 57 ist diese Folge periodisch; das erste Glied - die Null - wiederholt sich unendlich oft.

59. Wir führen als Beispiel die Folge $\widehat{F}_{11}^0$ an (Abb. B.25).

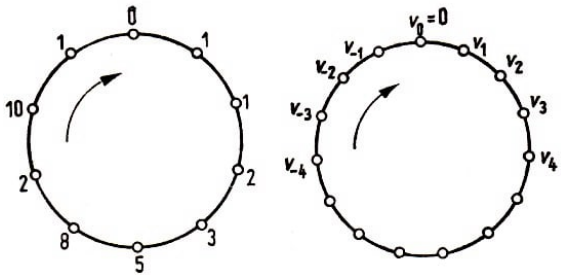


Abb. B.25,26

60. Wir bezeichnen das Element der Folge, das gleich Null ist, mit v_0 und nummerieren die übrigen Glieder so, wie es in Abb. B.26 gezeigt ist.
Wir überzeugen uns, dass folgende Gleichungen gelten:

$$v_0 + v_0 = 0, \quad v_1 - v_{-1} = 0, \quad v_2 + v_{-2} = 0, \quad v_3 - v_{-3} = 0, \quad v_4 - v_{-4} = 0, ...$$

Die erste Gleichung gilt offensichtlich; die zweite folgt daraus, dass

$$v_1 = v_{-1} + v_0 = v_{-1} + 0 = v_{-1}$$

ist. Unter Berücksichtigung von

$$v_0 + v_1 = v_2 \qquad , \qquad v_0 - v_{-1} = v_{-2}$$

und durch Addition der ersten beiden Gleichungen erhalten wir die dritte Gleichung. Durch Addition der zweiten und dritten erhalten wir die vierte Gleichung, usw. Die bewiesenen Gleichungen können in folgende allgemeine Form gebracht werden:

$$v_n + (-1)^n v_{-n} = 0$$

61. Die Zahl $y = 0$ hat von den Zahlen x und z den gleichen Abstand. Daher gilt auf Grund von Aufgabe 60 entweder $x + z = 0$ oder $x - z = 0$. Da aber $x = 0$ ist, ist in beiden Fällen $z = 0$.

62. Die Nullen zerlegen $\widehat{F}_m$ in einige Bögen. Wir wählen aus diesen Bögen den kleinsten aus (falls es davon mehrere gibt, so nehmen wir einen beliebigen von ihnen) und bezeichnen mit x und y die an den beiden Endpunkten stehenden Elemente (beide sind gleich Null).
Wir wählen ein Element z derart, dass der Bogen $\widehat{yz}$ gleich dem Bogen $\widehat{xy}$ ist. Dann ist (siehe Aufgabe 61) $z = 0$.

Weiterhin verschieben wir im Uhrzeigersinn die Bögen $\widehat{zu}$, $\widehat{uv}$ usw., von denen jeder gleich $\widehat{xy}$ ist. Offensichtlich ist $u = v = ... = 0$.
Wenn Wir den ganzen Kreis noch einmal durchlaufen, müssen wir unvermeidlich entweder ins Innere des Bogens $\widehat{xy}$ gelangen oder an sein Ende x. Im Innern des Bogens $\widehat{xy}$ sind jedoch keine Nullen mehr enthalten. Deshalb können wir nur an seinen Endpunkt x gelangen.

Somit zerlegen die Nullen x, y, z, u, v, ... die Folge in gleiche Teile. Da der Abstand zwischen zwei Nullen nicht kleiner als der Bogen $\widehat{xy}$ ist, enthält F_m keine anderen Nullen als x, y, z, u, v, ...

63. Die Folge F_m^0, besteht aus den Resten der Glieder von F^0 nach der Division durch m, infolgedessen entsprechen die Nullen in F_m^0, den durch m teilbaren Gliedern von F^0 und umgekehrt. Der Folge F_m^0 entspricht die Kreisfolge $\widehat{F}_m^0$ die ihre Periode darstellt. Daher folgt die Aussage dieser Aufgabe aus Aufgabe 62.

64. Wenn $\widehat{F}_m$ die Null enthält und aus einer ungeraden Anzahl von Elementen besteht, so existiert darin ein Paar benachbarter Elemente x, y, die im gleichen Abstand von der Null liegen (Abb. B.27).

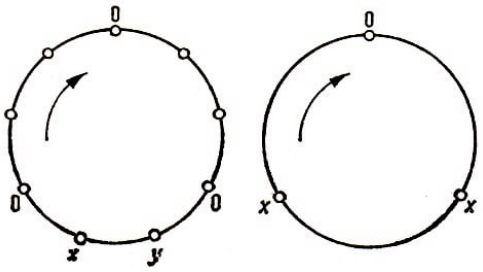


Abb. B.27,28

Auf Grund von Aufgabe 60 ist dann entweder $x + y = 0$ oder $x - y = 0$, und dann ist eines der Elemente der Folge, das an das Paar x, y angrenzt, gleich Null.
Gemäß Aufgabe 61 ist dann auch das andere dem Paar x, y benachbarte Element gleich Null. Daraus folgt $x = y$, und da die gesuchte Folge eine Folge ohne Wiederholungen ist, hat sie die in Abb. B.28 dargestellte Form.

65. Wir setzen voraus, dass die Kreisfolge wenigstens drei verschiedene Nullen enthält. Wir zeichnen drei aufeinanderfolgende Nullen aus und nummerieren sie im Uhrzeigersinn mit 0_1, 0_2, 0_3. Die Elemente der Folge, die jeweils vor diesen Elementen 0_1, 0_2, 0_3 stehen, bezeichnen wir mit u_1, u_2 bzw. u_3 und die Elemente, die jeweils auf 0_1, 0_2, 0_3 folgen, mit v_1, v_2, v_3 (Abb. B.29).

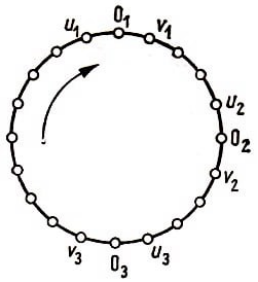


Abb. B.29

Offensichtlich gilt $u_1 = v_1$, $u_2 = v_2$ und $u_3 = v_3$. Da die Elemente u_1 und v_3 sich in gleichem Abstand von 0_2 befinden, gilt auf Grund von Aufgabe 60 entweder $u_1 + v_3 = 0$ oder $u_1 - v_3 = 0$. Aus der Gleichung $u_1 = v_3$ würden die Gleichungen $u_1 = v_1 = u_3 = v_3$ folgen, was aber unmöglich ist, weil die betrachtete Folge keine Wiederholungen enthält. Folglich gilt die Identität $u_1 = -v_3$ und die daraus folgende Gleichung

$$u_3 = -u_1 \tag{1}$$

Wir beweisen nun, dass $\widehat{F}_m$ eine Folge mit Wiederholungen ist, wenn sie genau drei Nullen enthält; denn die Nullen zerlegen im betrachteten Fall die Folge in drei gleiche Bögen, und man könnte ähnlich wie die Identität

$$u_3 = -u_1 \qquad \text{die Identitäten} \qquad u_1 = -u_2, \quad u_2 = -u_3$$

finden.
Aus diesen drei Identitäten folgt $u_1 = u_2 = u_3$, und das bedeutet, dass die betrachtete Folge eine Folge mit Wiederholungen ist.

Wir nehmen nun an, die Folge enthalte fünf verschiedene Nullen. Wir beweisen, dass auch in diesem Fall die Folge unbedingt Wiederholungen enthält. Wir bezeichnen fünf irgendwie aufeinanderfolgende Nullen der Reihe nach mit 0_1, 0_2, 0_3, 0_4, 0_5 und die ihnen im Uhrzeigersinn vorangehenden Elemente mit u_1, u_2, u_3, u_4, u_5 (Abb. B.30).

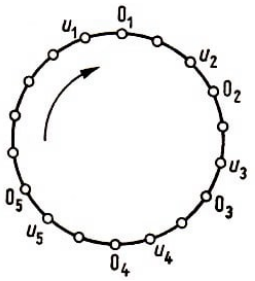


Abb. B.30

Wenden wir Formel (1) auf die verschiedenen Tripel von Nullen an, die sich aus den Elementen 0_1, 0_2, 0_3, 0_4, 0_5 bilden lassen, so erhalten wir

$$u_3 = -u_1, \quad u_4 = -u_2, \quad u_5 = -u_3$$

woraus $u_5 = u_1$ folgt; also enthält die Folge Wiederholungen.

66. a) Eine geometrische Progression mit dem Anfangsglied b und dem Quotienten q hat die Form

$$b, bq, bq^2, bq^3, ..., bq^{n-1}, bq^n, bq^{n+1}, ... \tag{1}$$

Diese Folge ist genau dann eine Fibonaccische Folge, wenn für alle n die Beziehung

$$bq^{n-1} + bq^n = bq^{n+1}$$

gilt. Diese Beziehung geht durch Kürzen mit bq^{n-1} in

$$1 + q = q^2 \qquad \text{oder} \qquad q^2 - q - 1 = 0 \tag{2}$$

über. Als Lösung dieser quadratischen Gleichung für q erhalten wir[36]

$$q = \frac{1 \pm \sqrt{5}}{2} \tag{3}$$

In der Arithmetik modulo 11 ist $\sqrt{5} = \pm 4$. Daher ist

$$q_1 = \frac{1+4}{2} = 8 \qquad , \qquad q_2 = \frac{1-4}{2} = 4$$

Setzt man diese Werte für q in (1) ein, so erhält man zwei Arten (Scharen) geometrischer Progressionen, die gleichzeitig Fibonaccische Folgen sind:

1. $b, 8b, 9b, 6b, 4b, 10b, 3b, 2b, 5b, 7b, b, ...,$
2. $b, 4b, 5b, 9b, 3b, b, 4b, 5b, 9b, 3b, b, ...$

b) In der Arithmetik modulo 7 lässt sich $\sqrt{5}$ nicht ziehen; daher hat die Gleichung (3) keine Lösung. Folglich existiert in der Arithmetik modulo 7 keine geometrische Progression, die gleichzeitig Fibonaccische Folge ist.

67. In der vorhergehenden Aufgabe wurden alle Folgen gefunden, die gleichzeitig geometrische Progressionen und Fibonaccische Folgen sind.
Es wurde festgestellt, dass diese Folgen in zwei Familien zerfallen. Wir wählen nun aus der ersten Familie eine Folge mit dem Anfangsglied x und aus der zweiten Familie eine Folge mit dem Anfangsglied y, addieren entsprechende Glieder und erhalten

$$\begin{aligned} &x+y, \quad 8x+3y, \quad 9x+5y, \quad 6x+9y, \quad 4x+3y, \quad 10x+y, \\ &3x+4y, \quad 2x+5y, \quad 5x+9y, \quad 7z+3y, \quad x+y, \quad ... \end{aligned} \tag{1}$$

das ist, wie man leicht sieht, wieder eine Fibonaccische Folge. Wir wählen nun x und y so, dass das erste Glied dieser Folge gleich Null wird und das zweite Glied gleich Eins. Als Lösung des Gleichungssystems

$$x + y = 0 \qquad , \qquad 8x + 4y = 1$$

finden wir

$$x = \frac{1}{4} = 3 \qquad , \qquad y = -3 = 8$$

Somit ergibt sich die Zerlegung der Fibonaccischen Folge nach der Formel

$$\begin{aligned} &c_0 = 0 = 3 + 8, \quad c_1 = 1 = 3 \cdot 8 + 8 \cdot 4, \quad c_2 = 1 = 3 \cdot 8^2 + 8 \cdot 4^2, \quad ..., \\ &c_n = 3 \cdot 8^n + 8 \cdot 4^n, \quad ... \end{aligned}$$

68. Wir wiederholen in allgemeiner Form die Überlegungen, die wir bereits für einen Spezialfall bei der Lösung der Aufgaben 66 und 67 angestellt haben. Der Quotient q einer geometrischen Progression, die zugleich eine Fibonaccische Folge ist, muss der

[36] Siehe Formel (3) in der Lösung der Aufgabe 25; wir erinnern daran, dass sie in der Arithmetik modulo 2 sinnlos wird.

quadratischen Gleichung $q^2 - q - 1 = 0$ genügen [siehe Formel (2) in der Lösung der Aufgabe 66].

a) Lässt sich $\sqrt{5}$ in der Arithmetik modulo p nicht ziehen, so hat die Gleichung (2) keine Lösung, woraus folgt, dass die gewünschte Fibonaccische Folge nicht existieren kann.
b) Lässt sich $\sqrt{5}$ ziehen, so liefert die Gleichung (2) zwei Werte für q, und jedem dieser Werte entspricht eine Familie geometrischer Progressionen, die gleichzeitig Fibonaccische Folgen sind:

$$1.\quad b, bq_1, bq_1^2, bq_1^3, ..., bq_1^n, ... \qquad , \qquad 2.\quad b, bq_2, bq_2^2, bq_2^3, ..., bq_2^n, ...$$

Die Folge

$$x + y, \quad xq_1 + yq_2, \quad xq_1^2 + yq_2^2, \quad ..., \quad xq_1^n + yq_2^2 n, \quad ... \tag{1}$$

ist wieder eine Fibonaccische Folge. Damit sich eine beliebige Fibonaccische Folge

$$v_0, v_1, v_2, ..., v_n, ... \tag{2}$$

in der Form (1) darstellen lässt, genügt es, x und y derart zu bestimmen, dass in den Folgen (1) und (2) die beiden Anfangsglieder übereinstimmen. Das lässt sich auf die Lösung des Gleichungssystems

$$x + y = v_0 \qquad , \qquad xq_1 + yq_1 = v_1$$

zurückführen. Als Lösung dieses Systems erhalten wir[37]

$$x = \frac{v_1 - v_0 q_2}{q_1 - q_2} \qquad , \qquad y = \frac{v_0 q_1 - v_1}{q_1 - q_2} \tag{2}$$

Damit wird die Zerlegung einer Fibonaccischen Folge in die Summe zweier geometrischer Progressionen durch die Formel

$$v_n = xq_1^n + yq_2^n \tag{4}$$

geliefert, wobei q_1 und q_2 die Wurzeln der Gleichung $q^2 - q - 1 = 0$ sind und x und y nach (3) berechnet wurden.

69. In einer Arithmetik modulo p gilt auf Grund von Aufgabe 15 die Gleichung $a^{p-1} = 1$ für jedes $a \neq 0$. Insbesondere ist $q_1^{p-1} = 1$ und $q_2^{p-1} = 1$, und aus Formel (4) der Lösung von Aufgabe 68 folgt

$$\begin{aligned} v_{p-1} &= xq_1^{p-1} + yq_2^{p-1} = x + y = v_0, \\ v_p &= xq_1^p + yq_2^p = xq_1 + yq_2 = v_1, \\ &... \\ v_{k+p-1} &= xq_1^{k+p-1} + yq_2^{k+p-1} = xq_1^k + yq_2^k = v_k \end{aligned}$$

[37] Gleichung (3) verliert ihren Sinn, wenn $q_1 = q_2$ ist. Damit dieser Spezialfall gilt, muss die Diskriminante der Gleichung $q^2 - q - 1 = 0$ gleich Null werden. Diese Diskriminante ist jedoch gleich 5 und kann nur in der Arithmetik modulo 5 verschwinden. Den Fall der Arithmetik modulo 5 haben wir jedoch ausgeschlossen.

70. Wir wählen ein beliebiges Element der Folge $\widehat{F}_p$ als Anfangspunkt und denken uns den Kreis, auf den wir unsere Folge geschrieben haben, unendlich oft im Uhrzeigersinn durchlaufen. Schreiben wir die Elemente ihrer Reihenfolge nach in eine Zeile, so erhalten wir eine unendliche periodische Folge $v_0, v_1, v_2, ..., v_n, ...$ eine Fibonaccische Folge F_p.

Auf Grund der vorhergehenden Aufgabe gilt $v_{p-1} = v_0$ und $v_p = v_1$. Da die ursprüngliche Kreisfolge eine Folge ohne Wiederholungen ist, werden wir niemals zwei gleichen Paaren benachbarter Elemente begegnen.
Daher entsprechen die gleichen Paare (v_0, v_1) und (v_{p-1}, v_p) ein und demselben Paar der Kreisfolge. Somit entspricht der aus $p-1$ Elementen bestehende Abschnitt $v_0, v_1, ..., v_{p-2}$ der Folge F_p dem Durchlaufen der Kreisfolge in einer ganzen Zahl von Umläufen.
Hieraus geht hervor, dass die Anzahl der Elemente der Kreisfolge durch die Zahl $p-1$ teilbar ist.

71. Als Beispiel führen wir die ersten 15 Glieder der Folge F_{11}^0 und der Quotientenfolge von F_{11}^0 an.

Folge F_{11}^0	0,	1,	1,	2,	3,	5,	8,	2,	10,	1,	0,	1,	1,	2,	3,	5,
Quotientenfolge	∞,	1,	2,	7,	9,	6,	3,	5,	10,	0,	∞,	1,	2,	7,	9,	

72. a) Die Zahlen einer Fibonaccischen Folge sind durch die Beziehung

$$v_n = v_{n-1} + v_{n-2}$$

verknüpft. Dividieren wir diese durch v_{n-1} und ersetzen wir $\frac{v_n}{v_{n-1}}$ durch t_n und $\frac{v_{n-1}}{v_{n-2}}$ durch t_{n-1} so erhalten wir die Formel

$$t_n = 1 + \frac{1}{t_{n-1}} \tag{1}$$

In der Folge $t_1, t_2, ..., t_n, ...$ treten nicht mehr als $p+1$ verschiedene Elemente auf, und zwar die p Zahlen der Arithmetik modulo p und das Symbol ∞. Daher kommen unter den Elementen dieser Folge unbedingt gleiche vor.
Aus allen Paaren gleicher Elemente wählen wir ein Paar von Elementen aus, die in der betrachteten Folge den kleinsten Abstand von- einander haben. Es seien dies die Elemente t_k und t_{r+k}. Dann sind r beliebige hintereinanderstehende Elemente der Folge $t_1, t_2, ..., t_n, ...$ paarweise voneinander verschieden. Zur vollständigen Lösung der Aufgabe bleibt noch zu zeigen, dass für jeden Wert von n die Identität $t_n = t_{r+n}$ gilt.

Uns ist bereits bekannt, dass sie für $n = k$ erfüllt ist:

$$t_k = t_{r+k} \tag{2}$$

Wir beweisen nun die Gleichungen

$$t_{k+1} = t_{r+k+1}, \quad t_{k+2} = t_{r+k+2}, \quad t_{k+3} = t_{r+k+3} \tag{3,4,5}$$

Dazu benutzen wir Formel (1). Nach dieser Formel ist

$$t_{k+1} = 1 + \frac{1}{t_k} \qquad , \qquad t_{r+k+1} = 1 + \frac{1}{t_{r+k}}$$

womit Gleichung (3) aus Gleichung (2) folgt. Ganz genauso findet man (4) aus (3), (5) aus (4) usw.
Man muss sich nun noch von der Gültigkeit der Gleichungen

$$t_{k-1} = t_{r+k-1}, \quad t_{k-2} = t_{r+k-2}, \quad ..., \quad t_1 = t_{r+1} \tag{6,7,8}$$

überzeugen. Wir lösen die Beziehung (1) nach t_{n-1} auf:

$$t_{n-1} = \frac{1}{t_n - 1}$$

Mit Hilfe dieser Formel leiten wir nacheinander (6) aus (2), (7) aus (6) usw. her, und zwar nach dem Verfahren, mit dem wir mit Hilfe der Formel (1) die Gleichungen (3), (4), (5), hergeleitet haben.

b) Wir konstruieren die Quotientenfolge von F_p^0. Die Folge F_p^0 beginnt mit den Elementen 0 und 1. Dementsprechend beginnt die Quotientenfolge mit dem Element ∞. Auf Grund von a) wiederholt sich das Symbol ∞ in der Quotientenfolge unendlich oft, und zwar jeweils in gleichen Abständen voneinander.
Wie man leicht sieht, entsprechen diese Elemente der Quotientenfolge den Nullen von F_p^0. Denen entsprechen wiederum die Elemente von F^0, die Vielfache von p sind.

73. Zunächst bemerken wir zweierlei:
1. Wenn die Quotientenfolgen

$$t_1, t_2, ..., t_n, ... \qquad , \qquad t'_1, t'_2, ..., t'_n, ... \tag{1,1'}$$

gleiche Anfangsglieder haben, so sind sie identisch, d.h., es gilt $t_n = t'_n$ für jedes n. Dies folgt aus der in Aufgabe 72a) abgeleiteten Formel.

2. Wenn in einer gewissen Quotientenfolge $t_1, t_2, ..., t_n, ...$ endlich viele Glieder am Anfang ausgelassen werden, so erhält man eine Folge $t_m, t_{m+1}, t_{m+2}, ..., t_n, ...$, die aus den gleichen Elementen wie die ursprüngliche Folge besteht.
In der Tat wiederholt sich auf Grund von Aufgabe 72a) jedes Element der Reihe $t_1, t_2, ..., t_n, ...$ unendlich oft; folglich kommen sie auch sämtlich in der Folge t_m, t_{m+1}, t_{m+2}, ..., t_n, ... vor. Die Umkehrung ist klar.

Wir nehmen nun an, es seien uns zwei beliebige Quotientenfolgen (1) und (1') gegeben, von denen uns bekannt ist, dass ein gewisses Element t_m von (1) einem gewissen Element t'_n von (1') entspricht. Wir betrachten die Folgen

$$t_m, t_{m+1}, t_{m+2}, ... \qquad \text{und} \qquad t'_n, t'_{n+1}, t'_{n+2}, ... \tag{2,2'}$$

Die Folgen (2) und (2') haben das gleiche Anfangsglied und sind daher gemäß Bemerkung 1. identisch. Außerdem besteht auf Grund von Bemerkung 2. die Folge (2) aus

den gleichen Elementen wie (1) und (2') aus den gleichen Elementen wie (1'). Folglich bestehen (1) und (1') aus den gleichen Elementen.

74. Die Formel aus der Aufgabe 51 kann für eine Folge F_p in die Form

$$v_n = c_{n-1}v_0 + c_n v_1$$

umgeschrieben werden. Unter Benutzung dieser Formel finden wir

$$t_{r+1} = \frac{v_{r+1}}{v_r} = \frac{c_r v_0 + c_{r+1} v_1}{c_{r-1} v_0 + c_r v_1}$$

Wir ersetzen c_{r+1} durch die Summe $c_{r-1} + c_r$, dividieren Zähler und Nenner des so umgewandelten Bruches durch $v_0 c_{r-1}$ und erhalten

$$t_{r+1} \frac{\frac{c_r}{c_{r-1}} + \left(1 + \frac{c_r}{c_{r-1}}\right)\frac{v_1}{v_0}}{1 + \frac{c_r}{c_{r-1}}\frac{v1}{v_0}}$$

Unter Berücksichtigung von $\frac{c_r}{c_{r-1}} = \overline{t}_r$ und $\frac{v_1}{v_0} = t_1$ ergibt sich die uns interessierende Formel

$$t_{r+1} = \frac{\overline{t}_r + (1 + \overline{t}_r)t_1}{1 + \overline{t}_r t_1} \tag{1}$$

Aus Gleichung (1) geht hervor:
1. Aus $\overline{t}_r = 0$ folgt $t_{r+1} = t_1$;
2. aus $t_{r+1} = t_r$, folgt $\overline{t}_r(t_1^2 - t_1 -) = 0$, und dann ist $\overline{t}_r = 0$ oder $t_1^2 - t_1 - 1 = 0$.

Es sei nun r die Länge der Periode der Folge $\overline{t}_1, \overline{t}_2, ..., \overline{t}_n, ...$, und t_1 sei nicht Wurzel der Gleichung $x^2 - x - 1 = 0$. Wir haben dann $\overline{t}_{r+1} = \overline{t}_1 = \infty$, und aus der Formel $\overline{t}_{r+1} = 1 + \frac{1}{\overline{t}_r}$ (siehe Aufgabe 72) folgt $\overline{t}_r = 0$.

Auf Grund der gleichen Aufgabe 72 sind die Elemente $\overline{t}_1, \overline{t}_2, ..., \overline{t}_r$ paarweise voneinander verschieden, insbesondere sind die Elemente $\overline{t}_1, \overline{t}_2, ..., \overline{t}_{r-1}$ verschieden von $\overline{t}_r = 0$. Gemäß 1. folgt aus der Identität $\overline{t}_r = 0$ die Identität $t_{r+1} = t_1$.
Hierbei sind alle Elemente $t_2, t_3, ..., t_r$ verschieden von t_1, da aus der Gleichung $t_1 = t_{s+1}$ $(s < r)$ die Identität $\overline{t}_s = 0$ folgen würde (gemäß 2.), was aber in Wirklichkeit nicht stimmt.
Damit ist gezeigt, dass die Länge der Periode von $t_1, t_2, ..., t_n, ...$ dieselbe ist wie die von $\overline{t}_1, \overline{t}_2, ..., \overline{t}_n, ...$ nämlich gleich r.

75. a) Wir betrachten zuerst den Fall, dass sich $\sqrt{5}$ in der Arithmetik modulo p nicht ziehen lässt. In dieser Arithmetik hat die Gleichung $x^2 - x - 1 = 0$ keine Lösung, und auf Grund von Aufgabe 74 haben alle Quotientenfolgen beliebiger F_p-Folgen Perioden der gleichen Länge r.

Die Elemente, die zu einer Periode einer Quotientenfolge gehören, sind paarweise voneinander verschieden (gemäß Aufgabe 72 a)). Daher existieren in jeder Quotientenfolge genau r verschiedene Elemente. Wir bezeichnen mit R_1 die Quotientenfolge, die der mit den Zahlen 0, 1 beginnenden Folge F_p^0 entspricht.

Das erste Glied von R_1 ist das Symbol ∞. Die Gesamtzahl der Elemente, die in der Quotientenfolge auftreten können, ist gleich $p+1$ (das Symbol ∞ und die p Zahlen aus der Arithmetik modulo p).

Wenn alle diese Elemente in der Folge R_1 vorkommen, ist $r = p+1$, und der Beweis ist erbracht.
Ist dies nicht der Fall, so wählen wir eine Zahl a, die in R_1 nicht enthalten ist, und betrachten die Fibonaccische Folge $1, a, ...$
Die entsprechende Quotientenfolge (wir wollen sie mit R_2 bezeichnen) beginnt mit der Zahl a. Gemäß Aufgabe 73 enthalten R_1 und R_2 keine gemeinsamen Elemente. Falls eine Zahl b aus der Arithmetik modulo p in keiner dieser Folgen enthalten ist, so konstruieren wir die Fibonaccische Folge $1, b, ...$

Die entsprechende Quotientenfolge (wir wollen sie mit R_3 bezeichnen) beginnt mit dem Element b und hat folglich sowohl mit R_1 als auch mit R_2 keine gemeinsamen Elemente.
Falls R_1, R_2, R_3 noch nicht alle Elemente $0, l, ..., p-1, \infty$ erschöpfen, so konstruieren wir eine vierte Folge R_4 usw., bis wir ein System von Folgen R_1, R_2, ..., R_k erhalten haben, das den gesamten Vorrat der möglichen Elemente erschöpft.
Dabei haben dann stets je zwei der so konstruierten Folgen kein Element gemeinsam. Jede von ihnen enthält genau r verschiedene Elemente. Hieraus folgt $p+1 = kr$, womit dieser Beweis beendet ist.

Es bleibt nun noch der zweite Fall zu betrachten, in dem sich $\sqrt{5}$ in der Arithmetik modulo p ziehen lässt. In diesem Restsystem hat die Gleichung $x^2 - x - 1 = 0$ die beiden Lösungen $\alpha = \frac{1+\sqrt{5}}{2}$ und $\beta = \frac{1-\sqrt{5}}{2}$.
Ist $p \neq 5$, so sind diese Lösungen voneinander verschieden. Aus der Beziehung $\alpha^2 - \alpha - 1 = 0$ folgt

$$\alpha^2 = \alpha + 1$$

Nach Division dieser Gleichung durch α erhalten wir

$$\alpha = 1 + \frac{1}{\alpha} \tag{1}$$

Erinnern wir uns nun an die Formel in Aufgabe 72 a), die es uns erlaubt, nacheinander die Glieder der Quotientenfolge zu berechnen, und setzen sie in die Formel (1) ein, so erkennen wir, dass die Quotientenfolge, die mit dem Element α beginnt, die Form

$$\alpha, \quad \alpha, \quad \alpha, ... \tag{2}$$

hat. Genauso hat die Quotientenfolge, die mit dem Element β beginnt; die Form

$$\beta, \quad \beta, \quad \beta, ... \tag{3}$$

Auf Grund von Aufgabe 74 haben alle übrigen Quotientenfolgen Perioden der gleichen Länge r. Nach der früheren Überlegung konstruieren wir ein System von Quotientenfolgen R_1, R_2, ..., R_k, die von den Folgen (2) und (3) verschieden sind, paarweise keine

gemeinsamen Elemente besitzen und außerdem insgesamt den ganzen Elementevorrat $0, 1, ..., p-1$ und ∞ (ohne α und β) erschöpfen.
Hieraus folgt die Gleichung $(p+1)-2 = kr$ oder $p-1 = kr$, d.h., r ist Teiler von $p-1$.

b) Die Reste der Glieder der gegebenen Folge bei der Division durch p bilden die Folge F_p^0,

$$c_0 = 0, \quad c_1 = 1, \quad c_2 = 1, ... \tag{4}$$

Wir konstruieren zu (4) die Quotientenfolge

$$\bar{t}_1 = \frac{c_1}{c_0} = \infty, \quad ..., \quad \bar{t}_n = \frac{c_n}{c_{n-1}} \tag{5}$$

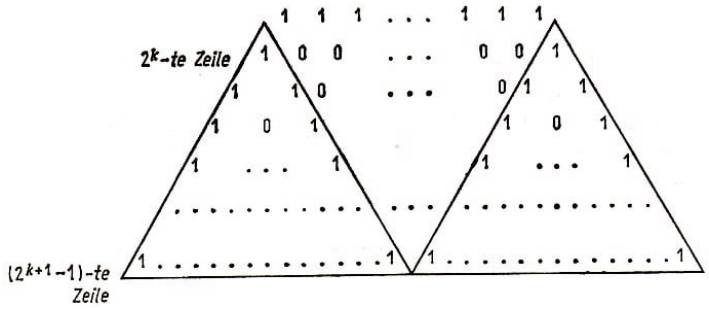
Zuerst nehmen wir an, dass sich $\sqrt{5}$ in der Arithmetik modulo p nicht ziehen lässt. Dann ist gemäß Aufgabe a) die Periodenlänge von (5) ein Teiler von $p+1$. Daher gilt $\bar{t}_{p+2} = \bar{t}_{1+(p+1)} = t_1 = \infty$, woraus $\frac{c_{p+2}}{c_{p+1}} = \infty$ und somit $c_{p+1} = 0$ folgen.

Das bedeutet, dass a_{p+1} durch p teilbar ist. Der Fall, dass sich $\sqrt{5}$ in der Arithmetik modulo p ziehen lässt, wird analog behandelt.

76. Der Teil des modulo 2 reduzierten Dreiecks, der aus den ersten neun Zeilen besteht (dabei ist die nullte Zeile mitgezählt), hat die Form

```
                1
              1   1
            1   0   1
          1   1   1   1
        1   0   0   0   1
      1   1   0   0   1   1
    1   0   1   0   1   0   1
  1   1   1   1   1   1   1   1
1   0   0   0   0   0   0   0   1
```

Hier sind in der zweiten, vierten und achten Zeile und nur in ihnen alle Glieder (mit Ausnahme der Randglieder) gleich Null. Unsere Behauptung sei bis zur 2^k-ten Zeile richtig (in diesem Fall besteht die (2^k-1)-te Zeile nur aus Einsen).
Wir zeigen, dass sie auch weiterhin richtig ist, d.h., dass die nächste Zeile, in welcher alle Glieder mit Ausnahme der Randglieder gleich Null sind, die 2^{k+1}-te Zeile ist:



Der gesamte Beweis ist in dem angeführten Schema enthalten. Wir empfehlen dem Leser, es genau zu betrachten, bevor er sich der ausführlichen Beweisführung zuwendet.

Von den beiden Randgliedern der 2^k-ten Zeile erzeugt jedes wieder ein dyadisches Pascalsches Dreieck, genau wie unser Ausgangsdreieck (das neue Dreieck entsteht aus dem ursprünglichen durch Parallelverschiebung).
Diese neuen Dreiecke (im Schema sind sie eingerahmt) erstrecken sich so weit nach unten, bis ihre Grundlinien zusammenstoßen. Dies ist dann eine Zeile mit der Nummer $2^k + h$, die aus zwei gleichen Teilen besteht, und zwar aus den h-ten Zeilen der beiden neuen Dreiecke.

In der $(2^k + h)$-ten Zeile des Pascalschen Dreiecks stehen $2^k + h + 1$ Elemente. In jeder h-ten Zeile der neuen Dreiecke stehen $h + 1$ Glieder. Daher gilt

$$2^k + h + 1 = 2(h + 1) \qquad , \qquad h = 2^k - 1$$

Somit schließen sich die $(2^k - 1)$-ten Zeilen der neuen Dreiecke. Jedoch ist die $(2^k - 1)$-te Zeile eines neuen Dreiecks identisch mit der $(2^k - 1)$-ten Zeile des ursprünglichen Dreiecks, welche gemäß unserer Induktionsvoraussetzung nur aus Einsen bestand.
Daher besteht die Zeile mit der Nummer

$$2^k + 2^k - 1 = 2^{k+1} - 1$$

unseres ursprünglichen Dreiecks ebenfalls nur aus Einsen. Folglich besteht die auf diese Zeile folgende 2^{k+1}-te Zeile nur aus Nullen (mit Ausnahme der Randglieder).
Außerdem befindet sich so lange, bis die neuen Dreiecke zusammenstoßen, d.h. bis zur 2^{k+1}-ten Zeile, im Innern jeder Zeile des ursprünglichen Dreiecks mindestens eine Eins (beispielsweise das Randglied der entsprechenden Zeile eines der neuen Dreiecke).

77. Die Dreiecke $\triangle_n^0$, $\triangle_n^1$, ..., $\triangle_n^k$, ..., $\triangle_n^n$ füllen den n-ten Streifen aus.
Für die ersten Streifen lässt sich unsere Behauptung leicht nachprüfen. Nehmen wir an, sie sei bis zum n-ten Streifen richtig; wir beweisen, dass sie dann auch weiterhin gilt.

Der Beweis basiert auf folgendem Hilfssatz: Im Pascalschen Dreieck seien zwei Gruppen von Zahlen ausgezeichnet, zum Beispiel $a_1, a_2, ..., a_r$ und $b_1, b_2, ..., b_r$ und jede von ihnen fülle lückenlos einen Teil irgendeiner Zeile aus. Wenn sich dann die beiden Gruppen nur um einen Faktor voneinander unterscheiden, d.h., wenn $b1 = ca_1$, $b_2 = ca_2$, ..., $b_r = ca_r$ ist, so unterscheiden sich auch die von ihnen erzeugten Dreiecke $a_1 a_r a$ und $b_1 b_r b$

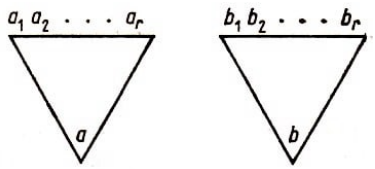


Abb. B.31

(Abb. 3.31) um denselben Faktor. Der Beweis des Hilfssatzes ist klar und folgt aus der Konstruktion des Pascalschen Dreiecks.

Wir betrachten das Dreieck $\triangle_n^k$ (Abb. 3.32). Da nach Voraussetzung unser Satz für den n-ten Streifen gültig war, ist $\triangle_n^k = P_n^k \cdot \triangle_0^0$.

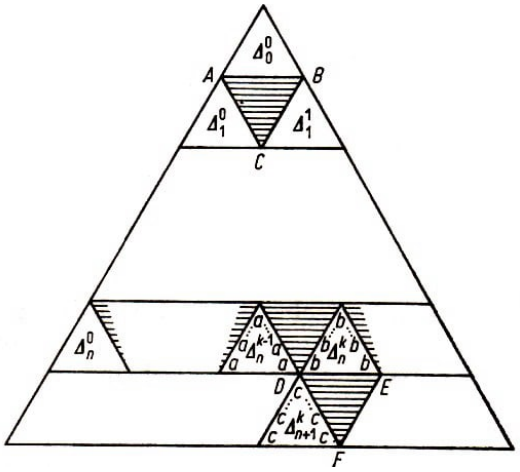


Abb. B.32

Insbesondere erhält man die letzte Zeile dieses Dreiecks aus der letzten Zeile des Dreiecks $\triangle_0^0$ durch Multiplikation mit P_n^k. Auf Grund des Hilfssatzes unterscheidet sich das Dreieck DEF von dem Dreieck ABC um denselben Faktor; ABC besteht jedoch aus lauter Nullen, daher enthält auch DEF nur Nullen.

Werden die Dreiecke $\triangle_n^{k-1}$ und $\triangle_n^k$, von den Zahlen a bzw. b und das Dreieck $\triangle_{n+1}^k$ von der Zahl c erzeugt, so ist $c = a + b$, daher ist auch

$$\triangle_{n+1}^k = \triangle_n^{k-1} + \triangle_n^k$$

(Abb. B.32). Außerdem gilt nach Voraussetzung $a = P_n^{k-1} \cdot 1 = P_n^{k-1}$, $b = P_n^k \cdot 1 = P_n^k$, also ist $c = P_n^{k-1} + P_n^k = P_{n+1}^k$ und

$$\triangle_{n+1}^k = P_{n+1}^k \triangle_0^0$$

Damit ist die Aufgabe vollständig gelöst.

78. Auf Grund der vorhergehenden Aufgabe enthält die s^2-te Zeile - die erste Zeile des s-ten Streifens - die oberen Eckpunkte der Dreiecke $\triangle_s^0$, $\triangle_s^1$, ..., $\triangle_s^s$; alle übrigen Glieder dieser Zeile sind gleich Null.
Es gilt jedoch $\triangle_s^k = P_s^k \cdot \triangle_0^0$, daher sind die Eckpunkte der Dreiecke $\triangle_s^k$ die Zahlen P_s^0, P_s^1, ..., P_s^{s-1}, P_s^s.

Nach Voraussetzung ist $P_s^1 = P_s^2 = ... = P_s^{s-1} = 0$.
Weiß man, dass alle inneren Glieder der s^2-ten Zeile gleich Null sind, so beweise man in der gleichen Weise unsere Behauptung für die s^3-te Zeile usw.

79. Wir führen den Beweis durch vollständige Induktion:
Für $n = 0$ gilt $(1 + x)^0 = 1 = C_0^0$,
für $n = 1$ gilt $(1 + x)^1 = 1 + x = C_1^0 + C_1^1 x$,
für $n = 2$ gilt $(1 + x)^2 = 1 + 2x + x^2 = C_2^0 + C_2^1 x + C_2^2 x^2$

Diese Formel sei für n bewiesen. Wir zeigen, dass sie dann auch für $n + 1$ Gültigkeit

besitzt. Es ist

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x) = (C_n^0 + C_n^1 x + C_n^2 x^2 + ... + C_n^{n-1}x^{n-1} + C_n^n x^n)(1+x) \\ &= C_n^0 + C_n^1 x + C_n^2 x^2 + ... + C_n^{n-1}x^{n-1} + C_n^n x^n \\ &+ C_n^0 x + C_n^1 x^2 + C_n^2 x^3 + ... + C_n^{n-1}x^n + C_n^n x^{n+1} \\ &(C_n^0 = C_n^n = 1 = C_{n+1}^0 = C_{n+1}^{n+1})\end{aligned}$$

Werden in einer in der gewöhnlichen Arithmetik gültigen Gleichung alle Zahlen durch ihren Rest bei der Division durch m ersetzt, so erhält man eine Gleichung, die in der Arithmetik modulo m gilt. Da P_n^k der Rest von C_n^k bei der Division durch m ist, folgt aus der in der gewöhnlichen Arithmetik richtigen Gleichung

$$(1+x)^n = C_n^0 + C_n^1 x + C_n^2 x^2 + ... + C_n^n x^n$$

die Richtigkeit der Gleichung

$$(1+x)^n = P_n^0 + P_n^1 x + P_n^2 x^2 + ... + P_n^n x^n$$

in der Arithmetik modulo m.

80. Auf Grund der vorhergehenden Aufgabe gilt

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

Andererseits folgt aus Aufgabe 15, dass in einer Arithmetik modulo einer Primzahl p für jedes x die Gleichungen $x^p = x$ und $(1+x)^p = 1 + x = 1 + x^p$ gelten. Daher gilt

$$(1+x)^p - (l + x^p) = 0 = P_p^1 x + P_p^2 x^2 + ... + P_p^{p-1}x^{p-1}$$

für jedes x. Das Polynom $(p-1)$-ten Grades $P_p^1 x + P_p^2 x^2 + ... + P_p^{p-1}x^{p-1}$ hat p Nullstellen $(x = 0, 1, ..., p-1)$; gemäß Aufgabe 33 sind alle Koeffizienten des Polynoms gleich Null, d. h.

$$P_p^1 = P_p^2 = ... = P_p^{p-1} = 0$$

was zu beweisen war.

81. Das Schema der Funktion $\dfrac{4x+1}{2x+3}$ ist aus Abb. 3.33 ersichtlich. Es besteht aus zwei Fixpunkten und drei Zyklen.

Abb. B.33

Das Schema der Funktion $\dfrac{2x+1}{3x+2}$ besteht nur aus zwei Zyklen und hat keine Fixpunkte.

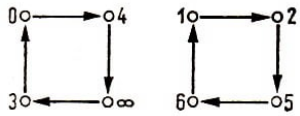


Abb. B.34

Das Schema der Funktion $\dfrac{3x-1}{x+1}$ (Abb. 3.35) besteht aus einem Fixpunkt und einem Zyklus.

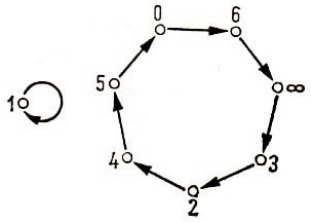


Abb. B.35

82. Das Schema für die Funktion $f^{-1}(x)$ erhält man aus dem Schema der Funktion $f(x)$, indem man in diesem die Richtungen aller Pfeile umkehrt.
Daher folgt die Behauptung der Aufgabe unmittelbar daraus, dass im Schema jeder gebrochenen linearen Funktion, d.h. auch für $f^{-1}(x)$, von jedem Punkt ein und nur ein Pfeil ausgeht.

83. Wörtlich wie in Aufgabe 15 a).

84. Es sei $n \neq \infty$ ein Fixpunkt der gebrochenen linearen Funktion $\dfrac{ax+b}{cx+d}$. Die Zahl n genügt dann der Gleichung

$$cx^2 + (d-a)x - b = 0 \tag{1}$$

denn es ist

$$\frac{an+b}{cn+d} = n, \qquad an+b = cn^2+dn, \qquad cn^2+(d-a)n-b = 0$$

Wir nehmen $c \neq 0$ an. Dann ist $f(\infty) = \frac{a}{c} \neq \infty$, d.h., ∞ ist kein Fixpunkt. Daher genügen alle Fixpunkte der Gleichung (1). Die quadratische Gleichung (1) kann für $c \neq 0$ jedoch nicht mehr als zwei Wurzeln haben (siehe Aufgabe 25). In unserem Fall hat sie aber mindestens drei Wurzeln. Folglich ist der Fall $c \neq 0$ unmöglich.

Es ist also $c = 0$. Der Punkt ∞ geht in sich über: $f(\infty) = \frac{a}{0} = \infty$. Die übrigen Fixpunkte (es gibt wenigstens zwei) müssen der Gleichung (1) genügen, die jetzt die Form

$$(d-a)x - b = 0 \tag{2}$$

hat. Nun hat aber die Gleichung (2) für $d-a \neq 0$ die einzige Wurzel $x = \frac{b}{d-a}$. Daher gilt $d-a = 0$. Hiernach ist $b = 0$, und unsere Funktion hat die Form $\frac{ax}{a} = x$, d.h., sie führt alle Punkte in sich über.

85. Es gilt

$$f(g(x)) = \frac{\frac{4x+3}{6x+3}+5}{5\frac{4x+3}{6x+3}+1} = \frac{6x+4}{5x+4}$$

$$g(f(x)) = \frac{4\frac{x+5}{5x+1}+3}{6\frac{x+5}{5x+1}+3} = \frac{5x+2}{5} = x+6$$

86. Die gesuchte Funktion ist $f(x) = 4x$. Man kann sie auf folgende Weise finden. Wir schreiben $f(x)$ in der allgemeinen Form

$$f(x) = \frac{ax+b}{cx+d}$$

und setzen für x nacheinander 0, 1 und 4 ein. Lösen wir die Bestimmungsgleichungen für a, b, c, d,

$$\frac{a\cdot 0+b}{c\cdot 0+d} = 0 \qquad , \qquad \frac{a\cdot 1+b}{c\cdot 1+d} = 4 \qquad , \qquad \frac{a\cdot 4+b}{c\cdot 4+d} = 2$$

auf, so erhalten wir $b = c = 0$, $a = 4d$, und die gesuchte Funktion hat die Form $f(x) = \frac{4dx}{d} = 4x$.

87. Die gesuchte Funktion habe die Form

$$f(x) = \frac{ax+b}{cx+d}$$

und keiner der Punkte x_1, x_2, x_3 sei gleich ∞. Nach Voraussetzung ist $f(x_1) = 0$, $f(x_3) = \infty$, d.h. $ax_1 + b = 0$, $cx_3 + d = 0$. Hiernach ist

$$b = -ax_1, \qquad d = -cx_3, \qquad ax+b = ax - ax_1 = a(x-x_1),$$
$$cx+d = cx - cx_3 = c(x-x_3)$$

und somit

$$\frac{ax+b}{cx+d} = \frac{a(x-x_1)}{c(x-x_3)}$$

Außerdem ist $f(x_2) = 1$, also

$$\frac{a(x_2-x_1)}{c(x_2-x_3)} = 1 \qquad , \qquad \frac{a}{c} = \frac{x_2-x_3}{x_2-x_1}$$

hieraus folgt

$$f(x) = \frac{x_2-x_3}{x_2-x_1}\cdot\frac{x-x_1}{x-x_3} = \frac{(x-2-x_3)x-(x_2-x_1)x_1}{(x_2-x_1)x-(x_2-x_1)x_3}$$

Für den Fall, dass einer der Punkte x_1, x_2, x_3 gleich ∞ ist, hat die gesuchte Funktion die Form

$$f(x) = \begin{cases} \frac{x_2-x_3}{x-x_3} & \text{für} \quad x_1 = \infty \\ \frac{x-x_1}{x-x_3} & \text{für} \quad x_2 = \infty \\ \frac{x-x_1}{x_2-x_1} & \text{für} \quad x_3 = \infty \end{cases}$$

wovon man sich leicht durch Einsetzen überzeugen kann.

88. Gemäß Aufgabe 87 existiert eine Funktion $f(x)$ derart, dass $f(y_1) = 0$, $f(y_2) = 1$, $f(y_3) = \infty$ ist. Die gebrochene lineare Funktion $f^{-1}(x)$ leistet das Gewünschte:

$$f^{-1}(0) = y_1, \qquad f^{-1}(1) = y_2, \qquad f^{-1}(\infty) = y_3$$

89. Es führe $f(x)$ die Werte x_1, x_2, x_3 in $0, 1, \infty$ und $\varphi(x)$ die Werte $0, 1, \infty$ in y_1, y_2, y_3 über (diese gebrochenen linearen Funktionen existieren auf Grund der Aufgaben 87 und 88).
Wir bilden die Funktion $\varphi(f(x))$. Es ist leicht einzusehen, dass diese Funktion die Werte x_1, x_2, x_3 in y_1, y_2, y_3 überführt.

Zwei gebrochene lineare Funktionen $g(x)$ und $h(x)$ mögen den Bedingungen

$$g(x_1) = y_1, \quad g(x_2) = y_2, \quad g(x_3) = y_3, \qquad h(x_1) = y_1, \quad h(x_2) = y_2, \quad h(x_3) = y_3$$

genügen. Wir wollen zeigen, dass $g(x)$ und $h(x)$ identisch sind. Es gilt

$$g^{-1}(y_1) = x_1, \quad g^{-1}(y_2) = x_2, \quad g^{-1}(y_3) = x_3,$$
$$g^{-1}(h(x_1)) = x_1, \quad g^{-1}(h(x_2)) = x_2, \quad g^{-1}(h(x_3)) = x_3$$

Die Funktion $g^{-1}(h(x))$ führt drei Punkte in sich über; auf Grund von Aufgabe 84 lässt sie aber dann alle Punkte fest, d.h., die Gleichung $g^{-1}(h(n)) = n$ gilt für jedes n.
Wenn aber $g^{-1}(x)$ die Zahl $m = h(n)$ in n überführt, dann führt $g(x)$ die Zahl n in $m = h(n)$ über, d.h., es ist $g(n) = h(n)$ für jedes n, was zu beweisen war.

90. Wir wählen ein Tripel voneinander verschiedener Punkte, beispielsweise $0, 1, \infty$. Jede gebrochene lineare Funktion führt dieses Punktetripel in ein anderes Tripel y_1, y_2, y_3 über.
Umgekehrt kann zu jedem Tripel voneinander verschiedener Punkte y_1, y_2, y_3 genau eine Funktion gefunden werden, die dieses Tripel in das Tripel $0, 1, \infty$ überführt.
Daher gibt es ebenso viele verschiedene gebrochene lineare Funktionen in einer Arithmetik modulo p, als es Tripel verschiedener Punkte in dieser um das Symbol ∞ erweiterten Arithmetik gibt (Tripel, die sich durch die Reihenfolge der Punkte unterscheiden, sind als verschieden anzusehen).

Als y_1 können wir jeden der $p + 1$ Punkte $0, 1, ..., p - 1, \infty$ wählen, als y_2 jeden der übrigen p Punkte und als y_3 schließlich jeden der restlichen $p - 1$ Punkte.
Es gibt also $(p+1)p(p-1)$ solcher Kombinationen, d.h., es gibt $(p+1)p(p-1)$ verschiedene Punktetripel und ebenso viele gebrochene lineare Funktionen in einer Arithmetik modulo p.

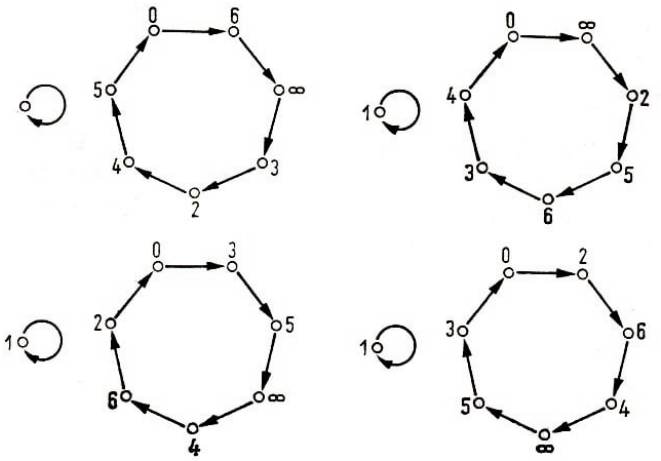


Abb. B.36-39

91. In Abb. B.36 ist das Schema der Funktion $f(x) = \dfrac{3x-1}{x+1}$ wiedergegeben. Die den Funktionen $f^2(x), f^3(x)$ und $f^4(x)$ entsprechenden Schemata sind in den Abb. B.37, B.38 und B.39 dargestellt.

92. Bei der Anwendung der Funktion $f^k(x)$ auf den Punkt x_0 rückt dieser um k Schritte auf seinem Zyklus weiter, und da k durch s teilbar ist, ergeben sich ganze Umläufe, d.h., der Punkt gelangt in seinen Ausgangspunkt zurück, also $f^k(x_0) = x_0$.

Ist umgekehrt der Punkt nach k Schritten in seine Ausgangslage zurückgekehrt, so bedeutet das, dass er seinen Zyklus eine gewisse Anzahl von Malen ganz durchlaufen hat, d.h., k ist durch s teilbar.

93. Es sei n ein Punkt, der durch $f^k(x)$ in sich übergeführt wird, durch $f(x) = \dfrac{ax+b}{cx+d}$ aber nicht, d.h. $f^k(n) = n$ und $f(n) \neq n$.
Gilt $f^k(n) = n$, so werden alle Punkte, die sich auf demselben Zyklus von $f(x)$ wie n befinden, durch $f^k(x)$ in sich übergeführt. Dies folgt sofort aus Aufgabe 92.
Hieraus folgt wiederum auf Grund von Aufgabe 84, dass $f^k(x)$ alle Punkte in sich überführt, wenn nur die Länge des Zyklus größer als 2 ist. Ganz analog wird der Fall behandelt, in dem die Länge des betrachteten Zyklus gleich 2 ist, die Funktion $f(x)$ aber wenigstens einen Punkt fest lässt.

Es bleibt nun noch der Fall zu betrachten, in dem $f(x)$ einen Zyklus von der Länge 2 hat und keinen Punkt in sich überführt. Wir berechnen die Funktion $f^2(x)$:

$$f^2(x) = \frac{(a^2+bc)x + ab + bd}{(ac+cd)x + bc + d^2}$$

Die Punkte unseres Zyklus werden durch $f^2(x)$ in sich übergeführt. Mindestens einer von ihnen ist nicht gleich ∞; dieser Punkt genügt den Gleichungen (siehe Lösung der Aufgabe 84)

$$\begin{aligned}(ac+cd)x^2 + (bc+d^2-a^2-bc)x - (ab+bd) &= 0\\ c(a+d)x^2 + (d-a)(d+a)x - b(a+d) &= 0\\ [cx^2 + (d-a)x - b](a+d) &= 0 \qquad (1)\end{aligned}$$

Ist $a+d \neq 0$, so ist $cx^2 + (d-a)x - b = 0$; das bedeutet jedoch (siehe Lösung der Aufgabe 84), dass x durch $f(x)$ in sich übergeführt wird, was aber im Widerspruch zu unserer Voraussetzung steht, wonach $f(x)$ keinen Punkt in sich überführen sollte. Daher ist $a+d=0$.

Dann genügen jedoch alle Zahlen der Gleichung (1), d.h., alle Punkte werden durch $f^2(x)$ in sich übergeführt, $f^2(x_0) = x_0$ für jedes x_0. Gemäß Aufgabe 92 haben alle Zyklen die Länge 2 (einen Zyklus mit der Länge 1, d. h. einen Fixpunkt, gibt es nicht).

Insbesondere liegen die Fixpunkte der Funktion $f(x)$ auch auf einem Zyklus der Länge 2, und k ist auf Grund von Aufgabe 92 eine gerade Zahl. Da die Länge jedes Zyklus ein Teiler von k ist, erhalten wir $f^k(n) = n$ für beliebiges n, was zu beweisen war.

94. Wir schließen alle Fixpunkte aus und betrachten unter den verbleibenden Zyklen einen Zyklus kleinster Länge r. Die Punkte dieses Zyklus werden durch die Funktion $f^r(x)$ in sich übergeführt. Daher führt auf Grund von Aufgabe 93 die Funktion $f^r(x)$ alle Punkte in sich über.
Wir wählen nun einen Zyklus, der aus mindestens zwei Gliedern besteht; seine Länge sei gleich s. Die Funktion $f^r(x)$ führt jeden seiner Punkte wieder in sich über, folglich ist (siehe Aufgabe 92) r durch s teilbar. Da stets $r \leq s$ ist, ist $r = s$. Somit ist die Länge jedes Zyklus gleich r.

95. Wenn wir den wenig interessanten Fall, in dem alle Punkte durch die Funktion $f(x)$ in sich übergeführt werden (in diesem Fall ist $x_{p+1} = x_p = x_{p-1} = x_0$), ausschließen, so werden durch die Funktion $f(x)$ entweder gar keine oder ein oder zwei Punkte in sich übergeführt (Aufgabe 84).
Die übrigen Punkte sind auf Zyklen mit gleicher Länge verteilt (Aufgabe 94); die Länge dieser Zyklen ist entsprechend den oben unterschiedenen Fällen entweder Teiler der Zahl $p + 1$ oder Teiler der Zahl p oder Teiler der Zahl $p - 1$.

Im ersten Fall ist $x_{p+1} = x_0$, im zweiten $x_p = x_0$ und im dritten $x_{p-1} = x_0$ (Aufgabe 92). Welcher dieser Fälle eintritt, hängt von der Anzahl der Fixpunkte ab.
Ist $c \neq 0$, so ist ∞ kein Fixpunkt, und die Anzahl der Fixpunkte ist gleich der Anzahl der Wurzeln der Gleichung (Aufgabe 84)

$$cx^2 + (d - a)x - b = 0$$

Auf Grund von Aufgabe 25 hat diese quadratische Gleichung keine Wurzel, wenn sich die Wurzel aus ihrer Diskriminante $(a - d)^2 + 4bc$ nicht ziehen lässt, eine Wurzel, wenn die Diskriminante gleich Null ist, und zwei Wurzeln, wenn die Diskriminante von Null verschieden ist und sich die Wurzel aus ihr ziehen lässt.
Für den Fall $c = 0$ überlassen wir dem Leser die Untersuchung.

Anmerkung. Die Quotientenfolge $t_1, t_2, ..., t_n, ...$ für die Fibonaccische Folge ist ein Spezialfall der allgemeinen Folge $x_0, x_1, ..., x_k, ...$ Hierbei sind $t_n = 1 + \frac{1}{t_{n+1}}$, $f(t) = 1 + \frac{1}{t} = \frac{t+1}{t}$, $a = b = c = 1$ und $d = 0$. Die Gleichung der Fixpunkte ist

$$x^2 - x - 1 = 0$$

Ihre Diskriminante ist gleich 5. Wir sehen, dass die Resultate der Aufgaben 74 und 75 a) Spezialfälle des allgemeinen Resultats für beliebige gebrochene lineare Funktionen sind.

96.
$$f(x) = \frac{x - 3}{x + 1}$$
$$f^2(x) = \frac{\frac{x-3}{x+1} - 3}{\frac{x-3}{x+1} + 1} = \frac{-x - 3}{x - 1}$$
$$f^3(x) = \frac{\frac{-x-3}{x-1} - 3}{\frac{-x-3}{x-1} + 1} = x$$

Die Funktion $f^3(x)$ lässt alle Punkte fest. Gemäß Aufgabe 92 ist die Zahl 3 teilbar durch die Länge jedes Zyklus der Funktion $f(x)$. Die Länge des Zyklus kann daher nur 1 oder 3 sein; nun führt aber die Funktion $f(x)$ nicht alle Punkte in sich über. Beispielsweise ist $f(\infty) = 1$. Daher haben nicht alle Zyklen die Länge 1, d.h., es existiert wenigstens ein Zyklus der Länge 3.

97. a) Wir betrachten die Funktion

$$f(x) = \frac{x-3}{x+1}$$

in der Arithmetik modulo p. Hier gilt

$$(a-d)^2 + 4bc = (1-1)^2 + 4(-3)\cdot 1 = 4(-3)$$

Im Restsystem lasse sich $\sqrt{-3}$ ziehen. Dann lässt sich auch

$$\sqrt{(a-d)^2 + 4bc} = \sqrt{4(-3)} = 2\sqrt{-3}$$

ziehen. Gemäß Aufgabe 95 gilt für jedes x_0 die Gleichung $f_{p-1}(x_0) = x_0$, insbesondere auch für solche x_0, die auf einem Zyklus mit der Länge 3 liegen (wie wir in Aufgabe 96 gesehen haben, existiert ein solcher Zyklus).
Es ist daher (Aufgabe 92) $p-1$ durch 3 teilbar, also $p-1 = 3k$, $p = 3k+1$.

Wir nehmen nun an, $\sqrt{-3}$ lasse sich in der Arithmetik nicht ziehen. Dann ist auch

$$\sqrt{(a-d)^2 + 4bc} = 2\sqrt{-3}$$

nicht lösbar, und es ist $f^{p+1}(x_0) = x_0$ für jedes $_0$. Hieraus folgt $p+1 = 3l$, $p = 3l-1 \neq 3k+1$.

b) Es sei p eine Primzahl und Teiler der Zahl a^2+3, ferner b der Rest bei der Division von a durch p. Dann gilt $b^2+3 = 0$, $b^2 = -3$, d.h., $\sqrt{-3}$ lässt sich in der Arithmetik ziehen. Hieraus schließen wir, dass $p = 3k+1$ ist.

Es sei nun $p = 3k+1$. Dann lässt sich $\sqrt{-3}$ in der Arithmetik modulo p ziehen, d.h., man kann eine Zahl a finden derart, dass $a^2+3 = 0$ in der Arithmetik modulo p gilt. Das bedeutet in der gewöhnlichen Arithmetik, dass a^2+3 durch p teilbar ist.

98.

$$f(x) = \frac{x-1}{x+1}$$

$$f^2(x) = \frac{\frac{x-1}{x+1} - 1}{\frac{x-1}{x+1} + 1} = -\frac{1}{x}$$

$$f^3(x) = \frac{-\frac{1}{x} - 1}{-\frac{1}{x} + 1} = \frac{-x-1}{x-1}$$

$$f^4(x) = \frac{\frac{-x-1}{x-1} - 1}{\frac{-x-1}{x-1} + 1} = x$$

Die Funktion $f^4(x)$ führt jeden Punkt in sich über. Gemäß Aufgabe 92 müssen die Längen der Zyklen von $f(x)$ Teiler der Zahl 4 sein, d.h., die Zyklen müssen die Länge 1, 2 oder 4 haben. Es haben nicht alle Zyklen die Länge 1, weil nicht alle Punkte durch die Funktion $f(x)$ in sich übergeführt werden, z.B. ist $f(0) = -1$.
Hätten alle Zyklen die Länge 1 oder 2, so würde die Funktion $f^2(x)$ alle Punkte in sich überführen. Das ist jedoch nicht der Fall, denn es ist

$$f^2(0) = \infty$$

Daher existiert mindestens ein Zyklus der Länge 4.

99. a) Wir betrachten in einer Arithmetik modulo p die Funktion

$$f(x) = \frac{x-1}{x+1}$$

Hierfür gilt

$$(a-d)^2 + 4bc = (1-1)^2 + 4(-1) \cdot 1 = 4(-1)$$

Wir nehmen an, $\sqrt{-1}$ lasse sich in der Arithmetik ziehen. Dann ist

$$\sqrt{(a-d)^2 + 4bc} = \sqrt{4(-1)} = 2\sqrt{-1}$$

lösbar. Nach Aufgabe 95 gilt $f^{p-1}(x_0) = x_0$ für jedes x_0, worunter sich Werte für x_0 befinden, die auf einem Zyklus der Länge 4 liegen (wie wir in Aufgabe 98 gesehen haben, existiert ein derartiger Zyklus). Es ist daher (Aufgabe 92) $p-1$ durch 4 teilbar, also $p-1 = 4k$, $p = 4k+1$.

$\sqrt{-1}$ lasse sich nicht ziehen, dann ist auch

$$\sqrt{(a-d)^2 + 4bc} = 2\sqrt{-1}$$

nicht lösbar, und $f^{p+1}(x_0) = x_0$ gilt für jedes x_0. Hieraus folgt $p+1 = 4l$, $p = 4l-1 \neq 4k+1$.

b) Zur Lösung dieser Aufgabe siehe die Lösung von Aufgabe 24b).

100. Die geometrische Progression

$$b, bq, bq^2, ..., bq^n, ...$$

ist dann und nur dann auch eine Fibonaccische Folge, wenn ihr Quotient q die Gleichung $q^2 - q - 1 = 0$ befriedigt (siehe Lösung der Aufgabe 66). Als Lösungen dieser quadratischen Gleichung erhält man (siehe Lösung der Aufgabe 47)

$$q_1 = \frac{1+\sqrt{5}}{2} \quad , \quad q_2 = \frac{1-\sqrt{5}}{2}$$

Eine Lösung existiert genau dann, wenn sich $\sqrt{5}$ in der Arithmetik modulo p ziehen lässt.

Ist p von 2 und 5 verschieden, so ist die Bedingung[38], dass $\sqrt{5}$ in der Arithmetik der p-adischen Zahlen auftritt, gleichbedeutend der Bedingung, dass sich $\sqrt{5}$ in der Arithmetik modulo p ziehen lässt.
Existiert $\sqrt{5}$, so erhalten wir zwei Familien von F_p-Folgen, die gleichzeitig auch geometrische Progressionen sind:

$$b, bq_1, bq_1^2, ..., bq_1^n, ... \qquad , \qquad b, bq_2, bq_2^2, ..., bq_2^n, ...$$

101. Die Lösung folgt aus Aufgabe 100 (vgl. mit Aufgabe 68).

102. Auf Grund der vorhergehenden Aufgabe kann man die F-Folge $u_0, u_1, ..., u_n, ...$ als Summe zweier geometrischer Progressionen darstellen, die Lösung folgt daher aus Aufgabe 45.

103. Wir schreiben die Folge 0, 1, 1, 2, 3, ... im p-adischen System. Auf Grund der vorhergehenden Aufgabe stimmen die letzten k Ziffern der Glieder a_0, und $a_{p^{k-1}(p-1)}$ überein. Von a_0 sind jedoch alle Ziffern Nullen ($a_0 = ...000$). Folglich sind auch die letzten k Ziffern von $a_{p^{k-1}(p-1)}$ Nullen. Das bedeutet aber, dass $a_{p^{k-1}(p-1)}$ durch p^k teilbar ist.

104. Wir prüfen diese Formel für die ersten Zeilen des Dreiecks:

$$\begin{array}{ccccc} & & C_0^0 = \frac{0!}{0!0!} = 1 & & \\ & C_1^0 = \frac{1!}{0!1!} = 1 & & C_1^1 = \frac{1!}{1!0!} = 1 & \\ C_2^0 = \frac{2!}{0!2!} = 1 & & C_2^1 = \frac{2!}{1!1!} = 2 & & C_2^2 = \frac{2!}{2!0!} = 1 \end{array}$$

Nun nehmen wir an, unsere Formel sei für die n-te Zeile erfüllt, und zeigen, dass sie dann auch für die $(n+1)$-te Zeile gilt. Wir schreiben uns die n-te und die $(n+1)$-te Zeile auf,

$$\begin{array}{cccccccc} & & & & C_n^0 & C_n^1 & ... & C_n^{k-1} \quad C_n^k \quad ...C_n^n \\ C_{n+1}^0 & C_{n+1}^1 & ... & C_{n+1}^{k-1} & C_{n+1}^k & C_{n+1}^{k+1} & ... & C_{n+1}^{n+1} \end{array}$$

und benutzen die Beziehung

$$C_{n+1}^k = C_n^{k-1} + C_n^k$$

Da nach Voraussetzung

$$C_n^{k-1} = \frac{n!}{(k-1)![n-(k-1)]!} = \frac{n!}{(k-1)!(n-k+1)!}$$
$$C_n^k = \frac{n!}{k!(n-k)!}$$

gilt, ist

$$\begin{aligned} C_{n+1}^k &= \frac{n!}{(k-1)!(n-k+1} + \frac{n!}{k!(n-k)!} = \frac{n!k}{k!(n-k+1)!} + \frac{n!(n-k+1)}{k!(n-k+1)!} \\ &= \frac{n!(k+n-k+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k![(n+1)-k]!} \end{aligned}$$

[38] Es wäre vielleicht besser, $\sqrt{...005}$ zu schreiben, um Verwechslungen mit $\sqrt{5}$ zu vermeiden, wobei 5 Element der Arithmetik modulo p ist.

Unsere Formel war für die nullte, erste und zweite Zeile gültig, folglich gilt sie, wie bewiesen, auch für die dritte Zeile, vierte Zeile usw., d.h., sie gilt für alle Zeilen. (Aus der bewiesenen Formel folgt unter anderem, dass $n!$ für jedes $k < n$ durch das Produkt $k!(n-k)!$ teilbar ist.)

105. Es ist

$$C_{p-k-1}^{k} = \frac{(p-k-1)!}{k!(p-2k-1)!} = \frac{(p-k-1)(p-k-2)...(p-2k)(p-2k-1)...1}{k!(p-2k-1)(p-2k-2)...1}$$
$$= \frac{(p-k-1)(p-k-2)...(p-2k)}{k!} = \frac{[p-(k+1)][p-(k+2)]...[p-2k]}{k!}$$

Es ist $k!$ nicht durch p teilbar wegen $k \leq \frac{p-1}{2} < p$, d.h. aber, dass $k!$ modulo p nicht gleich Null ist. Wir erhalten also in der Arithmetik modulo p die Gleichung

$$P_{p-k-1}^{k} = \frac{[-(k+1)][-(k+2)]...[-2k]}{k!} = \frac{(-1)^k(k+1)(k+2)...2k}{k!}$$
$$= (-1)^k \frac{(2k)!}{k!k!} = (-1)^k P_{2k}^{k}$$

106. Es ist $P_{2n}^{n} = \frac{(2n)!}{n!n!}$. Ferner gilt

$$(2n)! = 1 \cdot 2 \cdot 3...2n = 1 \cdot 3 \cdot 5...(2n-1) \cdot 2 \cdot 4 \cdot 6...2n$$
$$= 1 \cdot 3 \cdot 5...(2n-1) \cdot (2 \cdot 1) \cdot (2 \cdot 2)...(2 \cdot n) = 1 \cdot 3 \cdot 5...(2n-1) \cdot 2^n \cdot 1 \cdot 2 \cdot 3...n$$
$$= 2^n \cdot n! \cdot 1 \cdot 3 \cdot 5...(2n-1)$$

Demnach ist

$$P_{2n}^{n} = 2^n \frac{1 \cdot 3 \cdot 5...(2n-1)}{n!}$$

Andererseits gilt

$$1 \cdot 3 \cdot 5...(2n-1) = (-1)^n(-1)(-3)..[-(2n-1)] = (-1)^n(p-1)(p-3)...[p-(2n-1)]$$
$$= (-1)^n 2^n \left(\frac{p-1}{2}\right)\left(\frac{p-3}{2}\right)...\left(\frac{p-2n+1}{2}\right)$$
$$= (-1)^n 2^n \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}-1\right)...\left(\frac{p-1}{2}-n+1\right) = (-1)^n 2^n \frac{\left(\frac{p-1}{2}\right)!}{\left(\frac{p-1}{2}-n\right)!}$$

hieraus folgt

$$P_{2n}^{n} = (-1)^n 4^n \frac{\left(\frac{p-1}{2}\right)!}{n!\left(\frac{p-1}{2}-n\right)!} = (-4)^n P_{\frac{p-1}{2}}^{n}$$

107. Gemäß Aufgabe 106 ist

$$S = 1 + 2q + ... + P_{2n}^{n} q^n + ... + P_{p-1}^{\frac{p-1}{2}} q^{\frac{p-1}{2}}$$
$$= 1 - 4P_{\frac{p-1}{2}}^{1} q + ... + (-4)^n P_{\frac{p-1}{2}}^{n} q^n + ... + (-4)^{\frac{p-1}{2}} P_{\frac{p-1}{2}}^{\frac{p-1}{2}} q^{\frac{p-1}{2}}$$
$$= 1 + P_{\frac{p-1}{2}}^{1}(-4q) + ... + P_{\frac{p-1}{2}}^{n}(-4q)^n + ... + P_{\frac{p-1}{2}}^{\frac{p-1}{2}}(-4q)^{\frac{p-1}{2}} = (1-4q)^{\frac{p-1}{2}}$$

Ist $q \neq \frac{1}{4}$, so ist $1-4q \neq 0$ und $S^2 = (1-4q)^{p-1} = 1$ (Aufgabe 15), woraus $S = \pm 1$ folgt.
Ist jedoch $q = \frac{1}{4}$, so ist $1-4q = 0$ und $S = 0$.

108. Aus Abb. 3.11 ist ersichtlich, dass $b_{n-1} + b_n = b_{n+1}$ ist. Somit bilden die Zahlen b_n eine Fibonaccische Folge. Nun ist aber $b_1 = 1$, $b_2 = 1$, d.h., die Anfangsglieder der Fibonaccischen Folgen

$$a_1 = 1, a_2 = 1, a_3 = 2, ... \qquad , \qquad b_1, b_2, b_3, ...$$

sind identisch und somit auch die beiden Folgen insgesamt, d.h. $b_n = a_n$.

109. Wir wissen, dass a_n die Summe der Zahlen ist, die in der p-ten Diagonalen stehen. Durch Übergang zur Arithmetik modulo p erhalten wir

$$c_p = P_{p-1}^0 + P_{p-2}^1 + ... + P_{p-1-k}^k + ... + P_{p-1-\frac{p-1}{2}}^{\frac{p-1}{2}} = P_{p-1}^0 + P_{p-2}^1 + ... + P_{p-1-k}^k + ... + P_{\frac{p-1}{2}}^{\frac{p-1}{2}}$$

(Hier bricht die Summe ab; $P_{\frac{p-1}{2}}^{\frac{p-1}{2}}$ ist das letzte Glied der $\frac{p-1}{2}$-ten Zeile.)
Nun ist aber $P_{p-1-k}^k = (-1)^k P_{2k}^k$ (Aufgabe 105). Daher gilt

$$c_p = P_0^0 + P_2^1 + ... + (-1)^k P_{2k}^k + ... + (-1)^{\frac{p-1}{2}} P_{p-1}^{\frac{p-1}{2}}$$

Benutzen wir die bei der Lösung der Aufgabe 107 gefundene Formel und berücksichtigen wir, dass im gegebenen Falle $q = -1$ ist, so erhalten wir

$$c_p = (1 - 4(-1))^{\frac{p-1}{2}} = 5^{\frac{p-1}{2}}$$

110. Der Beweis erfolgt durch Induktion. Für $n = 2$ gilt offenbar

$$\begin{array}{ccc} d_0 & & d_1 \\ & d_0^{(1)} & \end{array}$$

$$d_0^{(1)} = d_0 + d_1 = C_1^0 d_0 + C_1^1 d_1$$

Unser Satz sei für n Zahlen bewiesen. Wir beweisen ihn für $n+1$ Zahlen. Dazu betrachten wir die Tabelle

$$\begin{array}{ccccccccccc} d_0 & & d_1 & & d_2 & ... & d_{n-2} & & d_{n-1} & & d_n \\ & d_0^{(1)} & & d_1^{(1)} & & & & d_{n-2}^{(1)} & & d_{n-1}^{(1)} & \\ & & d_0^{(2)} & & & & & & d_{n-2}^{(2)} & & \\ & & & ... & & & & ... & & & \\ & & & & d_0^{(n-1)} & & d_1^{(n-1)} & & & & \\ & & & & & d_0^{(n)} & & & & & \end{array}$$

Nach Induktionsvoraussetzung gilt

$$d_0^{(n-1)} = C_{n-1}^0 d_0 + C_{n-1}^1 d_1 + ... + C_{n-1}^{n-1} d_{n-1}$$
$$d_1^{(n-1)} = C_{n-1}^0 d_1 + ... + C_{n-2}^{n-1} d_{n-1} + C_{n-1}^{n-1} d_{n-1}$$

durch Addition dieser Gleichungen erhalten wir

$$d_0^{(n)} = d_0^{(n-1)} + d_1^{(n-1)} = C_n^0 d_0 + C_n^1 d_1 + ... + C_n^{n-1} d_{n-1} + C_n^n d_n$$

111. Wir beweisen, dass

$$(C_n^0)^2 + (C_n^1)^2 + ... + (C_n^n)^2 = C_{2n}^n$$

Auf die Tabelle

$$\begin{array}{ccccccccc} C_n^0 & & C_n^1 & & C_n^2 & ... & C_n^n \\ & C_{n+1}^1 & & C_{n+1}^2 & ... & C_{n+1}^n & \\ & & ... & & ... & & \\ & & & C_{2n}^n & & & \end{array}$$

wenden wir das Resultat von Aufgabe 110 an. Es gilt dann

$$d_0 = C_n^0, \quad d_1 = C_n^1, \quad ..., \quad d_n = C_n^n, \quad d_0^{(n)} = C_{2n}^{(n)}$$

Daher ist

$$C_{2n}^n = C_n^0 C_n^0 + C_n^1 C_n^1 + ... + C_n^n C_n^n = (C_n^0)^2 + (C_n^1)^2 + ... + (C_n^n)^2$$

112. Wir benutzen die Tabelle

$$\begin{array}{ccccccccccccccc} v_k & & v_{k+1} & & v_{k+2} & & v_{k+3} & ... & v_{k+p-2} & & v_{k+p-1} & & v_{k+p} \\ & v_{k+2} & & v_{k+3} & & v_{k+4} & & ... & & v_{k+p} & & v_{k+p+1} & \\ & & v_{k+4} & & v_{k+5} & & & ... & & & v_{k+p+2} & & \\ & & & ... & & & & & & ... & & & \\ & & & & & & & v_{k+2p} & & & & & \end{array}$$

In ihr steht unter jedem Paar benachbarter Zahlen deren Summe. Nun wenden wir das Resultat von Aufgabe 111 an. Dann ist

$$d_0 = v_k, d_1 = v_{k+1}, ..., d_p = v_{k+p}; \quad d_0^{(p)} = v_{k+2p}$$

In einer Arithmetik modulo p gilt

$$v_{k+2p} = P_p^0 v_k + P_p^1 v_{k+1} + ... + P_p^p v_{k+p}$$

Nun ist aber $P_p^0 = P_p^p ?1$ und $P_p^1 = P_p^2 = ... = P_p^{p-1} = 0$ (Aufgabe 80). Daher ist

$$v_{k+2p} = v_k + v_{k+p}$$

113. Die Glieder der F_p-Folge, deren Indizes durch p teilbar sind, bilden die Folge v_0, v_p, v_{2p}, ..., v_{np}, ... Setzen wir in der Formel aus Aufgabe 112 $k = (n-1)p$, so erhalten wir

$$v_{(n-1)p} + v_{np} = v_{(n+1)p}$$

114. Wir müssen m Klammerausdrücke miteinander multiplizieren:

$$\underbrace{(a+b)(a+b)...(a+b)}_{m-\text{mal}}$$

Werden die Klammern aufgelöst und die Glieder geordnet, so erhält am offenbar den Koeffizienten 1. Um $a^{m-1}b$ zu erhalten, muss man in einer der Klammern b und in allen übrigen Klammern a miteinander multiplizieren.
Es hat $a^{m-1}b$ daher den Koeffizienten m. Alle übrigen Glieder werden b in Potenzen enthalten, die nicht niedriger als 2 sind.

115. Für $l = 1$ gilt die Behauptung offenbar. Sie sei nun gültig für $l = s$; wir beweisen, dass sie dann auch für $l = s + 1$ gilt. Wir setzen $n = k$ und $m = ks$ in Aufgabe 52. Dann erhalten wir

$$a_{k(s+1)-1} = a_{k+ks-1} = a_{k-1}a_{ks-1} + a_k a_{ks}$$

Da a_k durch d teilbar ist und $a_0 = 0$ ebenfalls, ist gemäß Aufgabe 63 auch a_{ks} durch d teilbar. Daher ist das Produkt $a_k a_{ks}$ durch d^2 teilbar und

$$a_{k(s+1)-1} = a_{k-1}a_{ks-1} + xd^2 \tag{1}$$

wobei x eine ganze Zahl ist. Laut Voraussetzung gilt

$$a_{ks-1} = a_{k-1}^s + yd^2 \tag{2}$$

Durch Einsetzen von (2) in (1) erhalten wir

$$a_{k(s+1)-1} = a_{k-1}a_{k-1}^s + d^2(ya_{k-1} + x) = a_{k-1}^{s+1} + zd^2$$

d.h., $a_{k(s+1)-1} - a_{k-1}^{s+1}$ ist durch d^2 teilbar. Genauso beweist man, dass $a_{kl+1} - a_{k+1}^l$ den Teiler d^2 besitzt.

116. Nach Voraussetzung ist $a_k x m^n$, wobei x eine ganze Zahl ist. Hieraus folgt

$$a_{k+1} = a_{k-1} + a_k = a_{k-1} + xm^n \qquad , \qquad a_{k+1}^m = (a_{k-1} + xm^n)^m$$

Gemäß Aufgabe 114 ist

$$(a_{k-1} + xm^n)^m = a_{k-1}^m + ma_{k-1}^{m-1}xm^n + x^2m^{2n}S = a_{k-1}^m + m^{n+1}(a_{k-1}^{m-1}x + x^2m^{n+1}S)$$

Daher ist $a_{k+1}^m - a_{k-1}^m$ durch m^{n+1} teilbar.

117. Nach Aufgabe 115 (wenn man $d = m^n$ setzt) gilt

$$a_{km+1} = a_{k-1}^m + xm^{2n} \qquad , \qquad a_{km-1} = a_{k-1}^m + ym^{2n}$$

Auf Grund der vorhergehenden Aufgabe ist $a_{k+1}^m - a_{k-1}^m$ durch m^{n+1} teilbar, also ist auch die Differenz $a_{km+1} - a_{km-1} = a_{km}$ durch m^{n+1} teilbar.

118. Die Lösung folgt aus der vorhergehenden Aufgabe. Ist a_k durch m teilbar, so ist a_{km} durch m^2 teilbar, dann ist jedoch a_{km^2} durch m^3 teilbar usw., $a_{km^{n-1}}$ durch m^n teilbar.
Nach Aufgabe 63 sind alle Glieder $a_{km^{n-1}s}$ durch m^n teilbar, wenn $a_{km^{n-1}}$ durch m^n teilbar ist.

119. Wegen $a-c=(d-b)\sqrt{5}$ müsste die ganze Zahl $a-c$ gleich der irrationalen Zahl $(d-b)\sqrt{5}$ sein. Dieser Widerspruch entfällt nur für $d-b=0$, woraus auch $a-c=0$ folgt. Also ist $a=c$, $b=d$.

120. Es gilt

$$(a+b\sqrt{5})(c+d\sqrt{5})=ac+bc\sqrt{5}+ad\sqrt{5}+5bd=(ac+5bd)+(ad+bc)\sqrt{5}$$

Die zweite Aussage der Aufgabe folgt unmittelbar aus dieser Formel.

121. Unter Benutzung der Lösung von Aufgabe 120 erhalten wir

$$m+n\sqrt{5}=(ac+5bd)+(ad+bc)\sqrt{5}$$

Nach Aufgabe 119 ist $m=ac+5bd$ und $n=ad+bc$. Daher gilt

$$\begin{aligned} m-n\sqrt{5}&=(ac+5bd)-(ad+bc)\sqrt{5}=[ac+5(-b)(-d)]+[a(-d)+(-b)c]\sqrt{5}\\ &=(a-b\sqrt{5})(c-d\sqrt{5}) \end{aligned}$$

122. a) Wenn $a^2-5b^2=1$ ist, so gilt auch $a^2-5(-b)^2=1$, d.h.,

$$a+(-b)\sqrt{5}=a-b\sqrt{5}$$

ist ebenfalls Lösung der Gleichung (1).
b)

$$\frac{1}{a+b\sqrt{5}}=\frac{a-b\sqrt{5}}{(a+b\sqrt{5})(a-b\sqrt{5})}=\frac{a-b\sqrt{5}}{a^2-5b^2}=a-b\sqrt{5}$$

123. a) Da nach Voraussetzung

$$m+n\sqrt{5}=(a+b\sqrt{5})(c+d\sqrt{5})$$

gilt, ist nach Aufgabe 121

$$m-n\sqrt{5}=(a-b\sqrt{5})(c-d\sqrt{5})$$

Daraus folgt

$$\begin{aligned} m^2-5n^2&=(m+n\sqrt{5})(m-n\sqrt{5})=(a+b\sqrt{5})(a-b\sqrt{5})(c+d\sqrt{5})(c-d\sqrt{5})\\ &=(a^2-5b^2)(c^2-5d^2)=1\cdot 1=1 \end{aligned}$$

b)

$$\frac{a+b\sqrt{5}}{c+d\sqrt{5}}=(a+b\sqrt{5})\frac{1}{c+d\sqrt{5}}=(a+b\sqrt{5})(c-d\sqrt{5})$$

Auf Grund von Aufgabe 122 a) ist $c-d\sqrt{5}$ Lösung der Gleichung (1).
Das Produkt $(a+b\sqrt{5})(c-d\sqrt{5})$ ist in der Form $p+q\sqrt{5}$ darstellbar (Aufgabe 120) und somit Lösung der Gleichung (1) (Aufgabe 123 a)).

124. $9^2 - 5 \cdot 4^2 = 1$; daher ist $9 + 4\sqrt{5}$ Lösung der Gleichung (1). Gemäß Aufgabe 123 a) ist auch

$$p_2 + q_2\sqrt{5} = (9 + 4\sqrt{5})(9 + 4\sqrt{5}) = (9 + 4\sqrt{5})^2$$

eine Lösung der Gleichung (1). Lösungen sind auch

$$p_3 + q_3\sqrt{5} = (p_2 + q_2\sqrt{5})(9 + 4\sqrt{5}) = (9 + 4\sqrt{5})^4$$

und allgemein

$$p_n + q_n\sqrt{5} = (9 + 4\sqrt{5})^n$$

für jede natürliche Zahl n. Alle diese Lösungen sind verschieden, da für $m \neq n$

$$(9 + 4\sqrt{5})^m \neq (9 + 4\sqrt{5})^n$$

125. Der Fall $a \geq c$ und $b \geq d$ ist ausgeschlossen, da sonst

$$a + b\sqrt{5} \geq c + d\sqrt{5}$$

wäre.
Daher gilt mindestens eine der beiden Ungleichungen $a < c$ oder $b < d$. Wir werden zeigen, dass aus der Gültigkeit einer dieser Ungleichungen die Gültigkeit der anderen folgt.
Es sei $a < c$. Dann ist auch $a^2 < c^2$ und

$$b^2 = \frac{a^2 - 1}{5} < \frac{c^2 - 1}{5} = d^2$$

woraus $b < d$ folgt, da $b \geq 0$ und $d \geq 0$ ist. Genauso gilt im Falle $b < d$

$$a^2 = 5b^2 + 1 < 5d^2 + 1 = c^2$$

also $a < c$.

126. a) Wir nehmen $a < 0$ an. Dann muss wenigstens eine der Zahlen $a + b\sqrt{5}$ und $a - b\sqrt{5}$ negativ sein (weil ihre Summe gleich $2a$, also negativ ist). Gleichzeitig ist aber ihr Produkt $(a + b\sqrt{5})(a - b\sqrt{5}) = a^2 + 5b^2 = 1$ positiv. Daher sind beide negativ im Widerspruch zu $a + b\sqrt{5} > 0$.

b) Wie eben gezeigt wurde, ist $a \geq 0$. Wir nehmen $b \leq 0$ an. Dann ist $-b \geq 0 \geq b$ und $a - b\sqrt{5} \geq a + b\sqrt{5} > 1$.
Hieraus folgt $1 = a^2 - 5b^2 = (a + b\sqrt{5})(a - b\sqrt{5}) > 1 \cdot 1 = 1$, womit wir zu einem Widerspruch gelangt sind.

127. Es existiere eine derartige Lösung. Aus Aufgabe 126 folgt dann, dass $a \geq 0$ und $b > 0$ sein muss. Nach Aufgabe 125 ist daher $a < 9$ und $b < 4$.
Es kann b somit nur die Werte 1, 2 und 3 annehmen. Man kann sich leicht davon überzeugen, dass keine der Zahlen $1 + 5b^2$, wobei $b = 1, 2, 3$ ist, ein vollständiges Quadrat ergibt; folglich ist die Zahl $a + b\sqrt{5}$ mit $b = 1, 2, 3$ keine Lösung der Gleichung (1).

128. Für $n = 0$ gilt $(9+4\sqrt{5})^0 = 1 = 1+0\sqrt{5}$, und für $n = 1$ ist $(9+4\sqrt{5})^1 = 9+4\sqrt{5}$, wobei $1 + 0\sqrt{5}$ und $9 + 4\sqrt{5}$ Lösungen der Gleichung (1) sind.

Für $n \geq 2$ liefert die Formel $(9 + 4\sqrt{5})^n$ das Produkt von Lösungen der Gleichung (1), d.h. wieder eine Lösung $p + q\sqrt{5}$, wobei $p \geq 0$ und $q \geq 0$ ist (Aufgabe 120).

Wir zeigen nun, dass unsere Formel die Gesamtheit der ganzzahligen Lösungen $p+q\sqrt{5}$ liefert, wobei $p \geq 0$ und $q \geq 0$ ist. Dazu nehmen wir das Gegenteil an.
Es sei $p + q\sqrt{5}$ mit $p \geq 0$ und $q \geq 0$ eine Lösung, die mit keinem Glied der Folge

$$(9 + 4\sqrt{5})^0, (9 + 4\sqrt{5})^1, (9 + 4\sqrt{5})^2, ..., (9 + 4\sqrt{5})^n, ...$$

identisch ist. Es ist ausgeschlossen, dass

$$p + q\sqrt{5} < (9 + 4\sqrt{5})^0 = 1 + 0 \cdot \sqrt{5}$$

ist (denn dann wäre $q < 0$ gemäß Aufgabe 125). Da die Glieder unserer Folge unbeschränkt wachsen, muss $p + q\sqrt{5}$ zwischen irgend zwei dieser Glieder liegen, d.h., es existiert ein $n \geq 0$ derart, dass

$$(9 + 4\sqrt{5})^n < p + q\sqrt{5} < (9 + 4\sqrt{5})^{n+1}$$

ist. Wir dividieren diese Ungleichung durch $(9 + 4\sqrt{4})^n$ und erhalten

$$1 < \frac{p + q\sqrt{5}}{(9 + 4\sqrt{5})^n} < 9 + 4\sqrt{5}$$

Nun ist $\dfrac{p + q\sqrt{5}}{(9 + 4\sqrt{5})^n}$ als Quotient zweier Lösungen der Gleichung (1) wieder eine Lösung der Gleichung (1). Wir erhalten somit eine Lösung der Gleichung (1), die zwischen 1 und $9 + 4\sqrt{5}$ liegt, was aber im Widerspruch zu Aufgabe 127 steht.

129. Ist $a + b\sqrt{5}$ eine Lösung der Gleichung (1), so sind offenbar auch

$$a - b\sqrt{5}, \quad -a + b\sqrt{5}, \quad -a - b\sqrt{5}$$

Lösungen der Gleichung (1). Nach Aufgabe 128 lässt sich eine dieser vier Zahlen in der Form $(9 + 4\sqrt{5})^n$ darstellen. Dann sind die übrigen drei in der Form

$$(9 + 4\sqrt{5})^{-n} = \frac{1}{(9 + 4\sqrt{5})^n}, \qquad -(9 + 4\sqrt{5})^n, \qquad -(9 + 4\sqrt{5})^{-n}$$

darstellbar.