IOLZ

ORIF

SAMMLUNG GÖSCHEN BAND 1131

Sammlung Göschen

Unser heutiges Wissen in kurzen, klaren, allgemeinverständlichen Einzeldarstellungen

Zweck und Ziel der „Sammlung Göschen" ist, in Einzeldarstellungen eine klare, leichtverständliche und übersichtliche Einführung in sämtliche Gebiete der Wissenschaft und Technik zu geben; in engem Rahmen, auf streng wissenschaftlicher Grundlage und unter Berücksichtigung des neuesten Standes der Forschung bearbeitet, soll jedes Bändchen zuverlässige Belehrung bieten. Jedes einzelne Gebiet ist in sich geschlossen dargestellt, aber dennoch stehen alle Bändchen in innerem Zusammenhange miteinander, so daß das Ganze, wenn es vollendet vorliegt, eine einheitliche, systematische Darstellung unseres gesamten Wissens bilden dürfte

Jeder Band in Leinen geb. RM 1.62
Sammelbezugspreise: 10 Exemplare RM 14.40, 25 Exemplare RM 33.75, 50 Exemplare RM 63.00

SAMMLUNG GÖSCHEN BAND 1131

EINFÜHRUNG IN DIE ZAHLENTHEORIE

Von

Dr. Arnold Scholz

Dozent der Mathematik an der Universität Kiel

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung · J. Guttentag, Verlagsbuchhandlung · Georg Reimer · Karl J. Trübner · Veit & Comp.

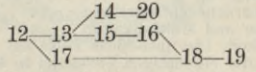
Berlin 1939

Archiv-Nr. 11 11 31

Druck von Walter de Gruyter & Co., Berlin W 35

Printed in Germany

Inhalt.

§-Abhängigkeit in III: 

Der Fermat-Satz läßt sich also bald nach Einführung der Kongruenzen entwickeln, ist aber auch für § 20 noch entbehrlich.

Weitere ausgewählte Literatur.

Dickson-Bodewig: Einführung in die Zahlentheorie. Leipzig 1931.

Dirichlet-Dedekind: Vorlesungen über Zahlentheorie. 3. Aufl. 1879; 4. Aufl. 1894. (Braunschweig.)

s. auch Dedekind, Ges. Werke.

Hecke: Vorlesungen über die Theorie der algebraischen Zahlen. Vgl. auch die Zeittafel am Ende des Buches. Leipzig 1923.

Hilbert: Bericht über die Theorie der algebraischen Zahlkörper. Jahresber. d. Dtsch. Math. Vgg. 4 (1894).

s. auch Hilbert, Ges. Werke.

Kraitchik: Théorie des nombres I. Paris 1922, II 1926. Récherches sur la . . .; 1924. (Öfters als Quelle verwandt.)

Im folgenden bringt der kleiner gedruckte Text Seitenbemerkungen und weitere Ausführungen; wer zum erstenmal Zahlentheorie treibt, mag ihn übergehen.

I. Die Arithmetik der natürlichen Zahlen.

§ 1. Einleitung.

Gegenstand der Zahlentheorie sind in erster Linie die natürlichen Zahlen 0, 1, 2, 3, 4 ..., zu einander in Beziehung gesetzt durch die beiden rationalen Hauptverknüpfungsarten, die Addition und die Multiplikation. Gerade die beschränkte Umkehrbarkeit dieser Operationen (Ausführbarkeit der Subtraktion und Division) im Bereich der natürlichen Zahlen liefert der Zahlentheorie ihr Arbeitsfeld. Insbesondere gilt dies für die Multiplikation, da die Frage, ob eine gegebene Zahl c durch eine gegebene Zahl a teilbar ist, d. h. ob es zu den Zahlen a und c eine Zahl x gibt, die die Gleichung $a \cdot x = c$ löst, nicht wie die entsprechende Frage der Addition schon durch die natürliche Anordnung der Zahlen entschieden ist. Die Frage der Teilbarkeit steht daher naturgemäß im Vordergrund der Zahlentheorie, und zwar sind in der klassischen Theorie alle Fragen mehr oder weniger vom Teilbarkeitsbegriff abhängig geworden, und man hat sich daran gewöhnt, bald mit dem „Ring" aller ganzen rationalen Zahlen (einschließlich der negativen) zu rechnen, in dem die Subtraktion stets eindeutig ausführbar bleibt. (Während die Algebra im Gegensatz zur Zahlentheorie gleich vom Körper aller rationalen Zahlen ausgeht, in dem auch die Division durch Zahlen verschieden von Null unbeschränkt eindeutig ausführbar ist.)

Wenn nun auch die Heranziehung der negativen ganzen Zahlen bei einem verhältnismäßig elementaren Zweig der Zahlentheorie wie der Darstellungstheorie der quadratischen Formen unentbehrlich ist und in der höheren Zahlentheorie (bei Bereichserweiterung vornehmlich durch algebraische Irrationalitäten) der Ringbegriff überhaupt grundlegend ist, so muß man auf der andern Seite beachten, daß fast alle elementar zahlentheoretischen Beweise aus geschickt vereinigter Verwendung vorhandener Anordnungen und Teilbarkeiten hervorgehn (Algorithmus) und auch in der höheren Zahlentheorie Normierungen durch natürliche Zahlen vorgenommen werden. Hinzukommt, daß in der neuesten Forschung die anzahlmäßig

arbeitende „additive Zahlentheorie“ stärker hervortritt, in der die Anordnung die Teilbarkeit verdrängt. Wir werden darum vorwiegend im natürlichen Zahlbereich arbeiten.

Wenn wir so bei der Untersuchung von Eigenschaften der natürlichen Zahlen zuerst mit der Arithmetik zusammengehen, so verfolgen wir doch nicht ihre Grundlegung, sondern nehmen insbesondere die Existenz der natürlichen Zahlenreihe als geordnete Menge mit den nachher geforderten kennzeichnenden Eigenschaften hin.

§ 2. Die natürliche Zahlenreihe.

Die natürliche Zahl läßt folgende konkrete, ursprüngliche Deutungen zu, an die wir uns gern halten: einmal als Anzahl einer endlichen Menge von Dingen (0 als Anzahl der „leeren Menge“), ferner als Ordnungszahlen der beim Abzählen der Menge entstehenden Ordnung der Dinge; wobei alle unterhalb ihrer Anzahl liegenden Zahlen als Ordnungszahlen verwandt werden, wenn man mit 0 zu zählen beginnt. Beide Deutungen aufnehmend brauchen wir folgende grundlegenden Sätze:

Satz 1 (vom kleinsten Element): Jede nicht leere Menge natürlicher Zahlen hat ein kleinstes Element.

Satz 2 (vom vollständigen Induktionsschluß). Erste Form: Folgt die Richtigkeit einer Behauptung für jede Zahl n unter der Voraussetzung, daß sie für alle n vorangehenden Zahlen richtig sei, so ist die Behauptung für alle natürlichen Zahlen richtig.

Zweite Form: Ist eine Behauptung für die Zahl 0 richtig, und folgt für jede weitere Zahl n ihre Richtigkeit aus der für die n vorangehende Zahl, so ist die Behauptung für alle n richtig.

Während diese Form des Induktionsschlusses den besonderen Nachweis für die Zahl 0 erfordert, ist dies bei der ersten Form als unmittelbarer Anwendung von Satz 1 nicht nötig, wenn der Beweis nicht ausdrücklich von der Existenz etwa k vorangehender Zahlen abhängig ist; dann müßte er für alle kleineren Zahlen als k besonders bewiesen werden. Es kann auch sein, daß der Induktionsschluß zwar nicht auf die Existenz vorangehender Werte, für die er richtig sei, zurückgreift, aber nur für $n \geqq m$ gilt; dann kann man wenigstens behaupten, daß auch der Satz für $n \geqq m$ richtig ist.

Satz 3 (von der Definition durch vollständige Induktion): Wird jeder Zahl n ein Ding $A(n)$ zugeordnet auf Grund einer für alle $m < n$ bereits vorliegenden Zuordnung $A(m)$, so gibt es genau eine Funktion F, die $F(n) = A(n)$ für alle n erfüllt. (Anwendung in § 11!)

Versteht man unter dem *Abschnitt von n* die Menge aller Zahlen unterhalb n, so gilt

Satz 4 (Anzahlsatz): Verschiedene Abschnitte der natürlichen Zahlenreihe haben eine verschiedene *Anzahl*, d. h. es lassen sich ihre Elemente auch außer der Reihenfolge nicht gegenseitig eindeutig zuordnen.

Satz 5 (Dirichletsches Schubfächerprinzip): Verteilt man n Dinge auf m Klassen, und ist $m < n$, so müssen, ob eine Klasse leer bleibt oder nicht, in irgendeiner Klasse wenigstens zwei Dinge vorkommen.

Diesen Sätzen liegen folgende Begriffsbildungen zugrunde:

Die *natürliche Zahlenreihe* Z definiert man als *geordnete Menge* 0, 1, 2, 3 . . . mit folgenden Eigenschaften:

A. Sie besitze ein erstes, allen vorangehendes Element 0.

B. Jedes ihrer Elemente besitze ein unmittelbar folgendes.

C. Jeder ihrer echten Abschnitte besitze ein letztes Element.

Dabei heißt eine Menge unter Einführung einer Beziehung $<$ („vor" oder „kleiner") geordnet, wenn in ihr zwischen je zwei verschiedenen Elementen a und b genau eine der Beziehungen $a < b$ oder $b < a$ besteht und mit $a < b$ und $b < c$ auch $a < c$ gilt. Die Schreibweise $a > b$ (a „hinter" oder „größer" b) bedeute nur $b < a$, $\neq$ Verschiedenheit, $\leqq$ kleiner oder gleich, $\geqq$ größer oder gleich.

Positiv heißt ein $a > 0$ (als Anzahl einer wirklichen Menge).

Abschnitt der Menge heiße jede Teilmenge, der mit irgend einem Element auch jedes kleinere angehört, *echter Abschnitt*, wenn sie weder leer noch die volle Menge ist.

Endlich heißt eine Menge, die auf einen echten Abschnitt der natürlichen Zahlenreihe abbildbar ist (abzählbar ist mit den Zahlen bis zu einer Zahl n). Sonst unendlich. Satz 4 läßt sich dann auch so aussprechen, daß eine endliche Menge nicht auf einen echten Teil von sich abbildbar ist, wobei unter *Abbild* immer eine gegenseitig eindeutige Zuordnung zu verstehen ist.

(An sich ist das eine Verschärfung von Satz 4, die aus ihm erst folgt, wenn man schon hat, daß die Abzählung der Menge mit diesem echten Teil begonnen werden darf, wie beim Beweis von Satz 5 gezeigt wird.)

Beweis für Satz 1: Für eine Menge T ist der Satz klar, wenn 0 zu T gehört. Sonst nehme man zu T alle Zahlen v hinzu, die wenigstens eine Zahl aus T übertreffen: $v > t$ für ein t aus T. Die so ergänzte Menge heiße V. Alle Zahlen, die nicht in V vorkommen, sind kleiner als die Zahlen aus V und bilden daher einen echten Abschnitt A von Z. Das auf A (auf alle a aus A) folgende Element q liegt in V, und da es nicht hinter einem t kommt, auch in T; q ist also kleinstes Element von T.

Folgerung 1: Ist E eine bei natürlichen Zahlen vorkommende Eigenschaft, so gibt es eine kleinste Zahl dieser Eigenschaft.

Folgerung 2: Ein für natürliche Zahlen behaupteter Satz ist entweder allgemein richtig, oder es gibt eine kleinste Zahl q, für die er falsch ist.

Satz 2 folgt jetzt so: Die Induktionsannahme erster Art ist, daß der Satz auch für q richtig, wenn wie oben für alle vorangehenden Zahlen. Also bleibt nur die Möglichkeit: allgemeinrichtig. Für den Induktionsschluß zweiter Art muß man wissen, daß der Satz für 0 richtig; dann kann man aus der Richtigkeit des Satzes für den vorhandenen Vorgänger von q wieder auf die Richtigkeit für q schließen.

Beweis für Satz 3: Die Definition führt für jedes n vorerst zu einer Funktion F_n, die für alle $m \leq n$ definiert ist durch

$$F_n(m) = A(m).$$

Bei festem m gilt diese Gleichung für jedes $n \geqq m$. Dieser gemeinsame Wert muß nun $F(m)$ werden, was durch die Festsetzung $F(m) = F_m(m)$ erreicht wird. (F entsteht durch „Verschmelzung" der F_n).

Als Anwendung hiervon der Nachweis, daß die Gestalt der Zahlenreihe Z durch die Forderungen A., B., C. festliegt, d. h. daß zwei geordnete Mengen Z', Z'', die A., B., C. erfüllen, unter Erhaltung ihrer Ordnung aufeinander abbildbar sind: man ordnet nach Abbildung eines echten Abschnittes von Z' auf einen Abschnitt von Z'' stets dem darauffolgenden Element von Z' das darauffolgende von Z'' zu, was nach B. wegen C. möglich, verschmelzt die Zuordnungen und zeigt mit Satz 1, daß auch kein Element von Z'' überbleibt.

Bemerkung: Die Eindeutigkeit der Gestalt von Z wurde in Satz 3 noch nicht verwandt; im Gegenteil braucht für das Verschmelzungsverfahren wie für Satz 1 und den Induktionsschluß erster Art nur eine *wohlgeordnete* Menge vorzuliegen, d. h. eine solche, die außer A. die in BC. enthaltene Eigenschaft D. hat, daß auf jeden echten Abschnitt unmittelbar ein Element folgt.

Beweis von Satz 4: Im gegenteiligen Fall gäbe es eine kleinste Zahl n, deren Abschnitt auf den einer kleineren Zahl m abbildbar

wäre. Sind sich in dieser Abbildung die letzten Abschnittselemente n' und m' zugeordnet, so entsteht durch ihre Streichung eine Abbildung des Abschnitts von n' auf den von $m' < n'$, gegen die Annahme, daß n die kleinste Zahl der Eigenschaft sei. War aber n' auf ein $m'' < m'$ abgebildet und dann auf m' ein $n'' < n'$, so vertausche man diese Zuordnungen und streiche wieder n', m'.

Man nennt dann bei einer endlichen Menge n die *Anzahl* ihrer Elemente, wenn sie auf den Abschnitt von n abbildbar ist.

Satz 5 folgt jetzt so: Bildet man die Dinge auf den Abschnitt von n ab und die Klassen so auf den Abschnitt von m, daß die nicht leerbleibenden Klassen vor den etwa leer bleibenden kommen, somit auf den Abschnitt einer Zahl $m' \leqq m$ abgebildet werden, so erhielte man für den Fall, daß in jeder Klasse höchstens ein Ding läge, dadurch eine Abbildung des Abschnittes von n auf den von m'.

Die Möglichkeit, in der Abzählung der Klassen die nichtleeren voranzustellen, folgt mit Induktion von $m - 1$ auf m Klassen: Liegt eine Abzählung $K_0, K_1, \ldots$ der m Klassen vor, so darf man annehmen, daß die ersten $m - 1$ Klassen bereits vorschriftgemäß untereinander geordnet sind. Dann sind es auch alle Klassen, falls die letzte leer ist; andernfalls vertausche man diese mit der ersten leeren Klasse.

Schließlich gilt noch, daß eine Teilmenge T einer endlichen Menge M wieder endlich ist; denn durch ihre Vorwegnahme in der Abzählung von M wird sie auf den Abschnitt einer Zahl m' abgebildet.

Eine Menge von Zahlen, die kleiner als eine feste Zahl n sind, ist also endlich.

§ 3. Addition und Multiplikation.

Wir wollen jetzt die beiden Hauptverknüpfungsarten der natürlichen Zahlen, Addition und Multiplikation, so definieren, daß sich die Grundregeln des Rechnens daraus ableiten lassen. Die *Summe* $m + n$ zweier Zahlen m und n definieren wir so:

Es sei $m + 0 = m$ und $m + 1$ die auf m folgende Zahl. Allgemein definieren wir $m + n$ durch vollständige Induktion: liegt $m + n'$ schon für alle $n' < n$ fest, so sei $m + n$ die auf alle $m + n'$ folgende Zahl. Einfacher nach dem zweiten Induktionsprinzip definiert:

$$(1) \qquad \begin{array}{c} m + n = (m + n') + 1 \quad \text{für} \quad n = n' + 1 \quad \text{oder} \\ m + (n + 1) = (m + n) + 1 . \end{array}$$

Das *Produkt* $m \cdot n$ oder mn definieren wir so:

(2) $m \cdot 0 = 0,\ m \cdot 1 = m,\ m \cdot 2 = m + m,$ allgemein
$m \cdot n = m \cdot n' + m$ für $n = n' + 1.$

Also bei schrittweisem Anwachsen des Multiplikators n als schrittweise wiederholte Addition des Multiplikanden m.

Für die Addition und Multiplikation gelten folgende Hauptrechenregeln

1. *Assoziativität der Addition*: $l + (m + n) = (l + m) + n$.

2. *Umkehrbarkeit der Addition*: Es gibt für $m \leqq n$ genau eine Zahl x, die die Gleichung $m + x = n$ erfüllt.

Wir schreiben dann x als *Differenz* $x = n - m$.

Für $n < m$ gibt es kein x.

3. *Vergleichbarkeit von Summen*: Es ist $l + r < m + n$, wenn $l \leqq m$ und $r < n$.

4. *Kommutativität der Addition*: $m + n = n + m$.

5. *Assoziativität der Multiplikation*: $l \cdot mn = lm \cdot n$.

6. *Distributives Gesetz*: $l(m + n) = lm + ln$. Für $m \geqq n$: $l(m - n) = lm - ln$.

7. *Vergleichbarkeit von Produkten*: Es ist $l \cdot r < m \cdot n$, wenn $0 < l \leqq m$ und $r < n$.

Insbesondere gilt also $mn > 0$ für $m > 0,\ n > 0$.

Die Umkehrbarkeit der Multiplikation, d. h. die Lösbarkeit der Gleichung $lx = m$, die „Teilbarkeit von m durch l", ist als eine Besonderheit zu betrachten, die uns vom nächsten § an vorwiegend beschäftigen wird. Jedoch gilt:

8. *Eindeutigkeit der Division*: Die Gleichung $lx = m$ besitzt für $l \neq 0$ höchstens eine Lösung. (Ist $l = 0$, so führt jedes x auf $m = 0$; es ist dann für $m \neq 0$ kein x, für $m = 0$ jedes x Lösung.)

9. *Kommutativität der Multiplikation*: $m \cdot n = n \cdot m$.

Beweise: Daß die Definition (1) dieselbe Addition liefert wie die vorangestellte Definition, folgt so: die Addition (1) könnte höchstens eine kleinere Summe liefern; dann müßte es einen kleinsten Summanden n der Art geben, und das führt sofort zum Widerspruch.

1. gilt für $n = 0$ und $n = 1$ laut Definition (1). Allgemein schließt man mit vollständiger Induktion von $n' < n$ auf n so: Es ist $(l + m) + n$ nach Definition die auf alle $(l + m) + n'$ folgende Zahl, während $l + (m + n)$ die auf alle $l + (m + n')$ folgende ist; denn $m + n$ folgt unmittelbar auf die Zahlen $m + n'$. Mit

$$l + (m + n') = (l + m) + n'$$

für $n' < n$ gilt also auch $l + (m + n) = (l + m) + n$.

2. Daß es nur ein die Gleichung $n = m + x$ lösendes x geben kann, folgt aus der ursprünglichen Definition der Addition: es ist danach $m + y > m + x$ für $y > x$. (x im Abschnitt von y.) Dann ist mit $m + 0 \leqq m + x$ aber m die kleinste aus m durch Addition hervorgehende Zahl. Ist dann $n' = m + x'$ darstellbar für $m \leqq n' < n$, so auch $n = m + x$ mit dem auf die x' folgenden x.

3. ist nur noch für $l < m$ zu beweisen. Ist x die Lösung der Gleichung $l + x = m$, so gilt

$$m + n = l + x + n \geqq l + n > l + r,$$

wenn man zeigt, daß $x + n \geqq n$ ist. Dies folgt so: ist es richtig für $n' < n$, so gilt $x + n > x + n' \geqq n'$, also $x + n > n'$ für alle $n' < n$ und damit $x + n \geqq n$.

4. Es ist $n + 0 = n$, aber auch $0 + n = n$, wie durch Induktion folgt. Es ist auch $1 + n = n + 1$, was für $n = 0$ richtig ist und für $n = n' + 1$ aus $1 + n' = n' + 1$ nach dem *zweiten* Induktionsprinzip so folgt:

$$1 + n = 1 + (n' + 1) = (1 + n') + 1 = n + 1.$$

Allgemein gilt für $n = n' + 1$, wenn $m + n' = n' + m$ als richtig bereits erkannt ist,

$$m + n = m + n' + 1 = n' + m + 1 = n' + 1 + m = n + m.$$

Nachdem nun die Reihenfolge der Summanden einer Summe als gleichgültig festgestellt ist, hat man für die einer Zahl $n > 0$ vorangehende Zahl die Schreibweise $n - 1$ zur Verfügung, die wir ursprünglich für die Lösung der Gleichung $1 + x = n$ gebrauchten. Auch haben wir jetzt für $m, n > 0$ nicht nur $m + n > m$, was aus 3. mit $l = m$, $r = 0$ folgte, sondern auch $m + n > n$.

Beweis von 5. und 6. durch Induktion für n.

7. kann auf die schärfere Form $lr < ln \leqq lm$ gebracht werden. Die erste Ungleichung folgt dann aus 3. mit (2), die zweite mit Induktion von $n - 1$ auf n:

$$ln = l(n - 1) + l \leqq m(n - 1) + m = mn.$$

Der Fall $r = 0$ liefert dann $mn > 0$ bei $m, n > 0$.

8. Ist $m = lx = ly$ bei $y > x$, so $l(y - x) = ly - lx = 0$ nach 6. und 3. und dann nach 7. ein Faktor 0, also $l = 0$.

9. ist klar für $n = 0$. Die Induktion gelingt von $n - 1$ auf n, wenn man $n \cdot m = (n - 1) \cdot m + m$ zeigt. Das ist nun wieder richtig für $m = 1$ und allgemein durch Induktion von $m - 1$ auf m aus (2) zu gewinnen.

Bemerkung: Eine rein anzahlmäßige Definition ist so möglich: Hat man eine Menge M von m Dingen und eine Menge N von n Dingen, so bedeute das Produkt mn die Anzahl der Kombinationen je eines Elementes aus M und N. (Vgl. die Anwendung in (7); man veranschauliche sich die so definierte Mulitiplikation mit ihren Rechenregeln durch Anordnung der Kombinationen in einem Rechteck!)

Man hat den Vorteil einer sofort kommutativ definierten Multiplikation, braucht jedoch zur Einordnung dieser Begriffsbildung in die Zahlenreihe den Anzahlsatz.

Nach Regel 9. darf man jetzt auch 6. und 7. mit vertauschten „Faktoren" schreiben.

Einführung der Potenz: Wie wir die Multiplikation als wiederholte Addition eingeführt haben, verwendet man für wiederholte Multiplikation abkürzenderweise die „Potenzierung":

$$a^n = a^{n-1} \cdot a,$$

begonnen mit $a^0 = 1$, $a^1 = a$, $a^2 = a \cdot a$, (Quadrat), $a^3 = a^2 \cdot a$ (Kubus). Es wird

10. $a^{m+n} = a^m \cdot a^n$

11. $a^{mn} = (a^m)^n$
$= a^{m^n} = a^{(m^n)}$ außer in besonderen Fällen.

Die Potenzierung ist also nicht assoziativ, ebensowenig kommutativ. Doch gilt wegen 9. noch ein distributives Gesetz

12. $(ac)^n = a^n \cdot c^n$.

Aufgaben: Man führe die Beweise von 10.—12. aus! Man führe den Induktionsbeweis für 5. und 6. aus! Man versuche die Multiplikation allein auf Grund der Wohlordnungsbedingungen A. und D. (s. S. 8 u.) ohne Heranziehung von B. zu definieren und 5.—7. so unter Verwendung des ersten Induktionsprinzips zu beweisen! Man beweise $l + (m - n) = (l + m) - n$, für $m \geqq n$! Ebenso $l - (m - n) = l - m + n$, wenn außerdem $l \geqq m - n$!

§ 4. Teilbarkeit. Die unendliche Folge der Primzahlen. Zermelos Beweis der eindeutigen Primfaktorenzerlegung.

Wir nennen die Zahl m durch die Zahl l teilbar oder ein Vielfaches von l, wenn die Gleichung $lx = m$ eine Lösung besitzt. Zugleich heißt l ein Teiler von m, geschrieben $l \mid m$, oder

eine in m aufgehende Zahl. 1 geht in allen Zahlen auf und ist nur durch sich teilbar, während 0 durch alle Zahlen teilbar ist und nur in sich aufgeht. Für alle $n > 1$ gilt ohne Zusammenfallen $1 \mid n \mid 0$.

Satz 6: Gilt zugleich $m \mid n$ und $n \mid m$, so ist $m = n$. Aus $l \mid m$ und $m \mid n$ folgt $l \mid n$.

Denn mit $n = mx$ und $m = ly$ gilt $n = lyx$; für $l = n$ wird dabei $yx = 1$, also $x = y = 1$ und $m = n$.

Im Bereich N der Zahlen $n > 1$ besteht jede Zerlegung $m = kl$ aus Faktoren k, l, die kleiner sind als ihr Produkt m. Wir stellen uns die Aufgabe, für eine gegebene Zahl n eine möglichst weitgehende Faktorenzerlegung vorzunehmen, also in möglichst viele kleine Faktoren. Wir teilen darum zuerst die Zahlen $n > 1$ in *Primzahlen*, die keine Zerlegung zulassen, und *zusammengesetzte* (zerlegbare) Zahlen ein. Für die Primzahlen ist unsere Aufgabe als gelöst zu betrachten. Im Bereich Z können wir sie auch so kennzeichnen:

Eine Primzahl p ist eine Zahl, die nur die beiden Teiler 1 und p besitzt. 1 zählt also nicht als Primzahl; sie wäre in einer Zerlegung doch unwesentlicher Faktor.

Wir wollen einen Teiler $t > 1$ einen wesentlichen Teiler nennen und einen Teiler $t < m$ von m einen echten Teiler. Es gilt dann der

Satz 7: Jede Zahl m aus N hat wenigstens einen Primteiler; nämlich der kleinste wesentliche Teiler q von m ist eine Primzahl. Denn aus $1 < p \mid q$ folgt $p \mid m$ mit $q \mid m$ und dann $p = q$.

Die Menge der Primzahlen, beginnend mit $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$, ist entweder endlich, d. h. auf einen echten Abschnitt der Zahlenreihe abbildbar, endigend mit einem p_n. Oder sie ist unendlich und auf die ganze Zahlenreihe abbildbar; es gibt dann, nach unserer Numerierung, zu jedem positiven n eine Primzahl p_n. Wir werden mit Euklid zeigen:

Satz 8: Es gibt unendlich viele Primzahlen.

Beweis: Ist q eine Primzahl, etwa $q = p_n$, so bilde man das Produkt $P = p_1 \cdot p_2 \cdots p_n$ der ersten n Primzahlen bis q. Der kleinste wesentliche Teiler von $P + 1$ ist dann eine neue Primzahl $r > q$. Denn da die Primzahlen $p_1, p_2, \ldots q$ in P

aufgehn und größer als 1 sind, gehen sie alle nicht in $P+1$ auf. Also gibt es mit r auch eine auf $q = p_n$ unmittelbar folgende Primzahl, was zu beweisen war. Es gilt nun der

Satz 9 (Fundamentalsatz): In N ist jede Zahl n eindeutig als Produkt von Primzahlen darstellbar:

$$n = p_1 p_2 \cdots p_s \quad (s \geqq 1). \tag{3}$$

Natürlich ist die Darstellung nur abgesehen von der Reihenfolge der Faktoren eindeutig. Man könnte etwa die Primfaktoren der Größe nach ordnen und bekäme dann eine Darstellung

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \tag{4}$$

mit $p_1 < p_2 < p_3 < \cdots < p_r$ und positiven Exponenten.

Die Existenz einer Zerlegung (3) folgt bereits aus Satz 7: Sind alle $m < n$ in Primfaktoren zerlegbar, so sei, wenn n nicht selbst Primzahl, p_1 sein kleinster Primteiler und $n = p_1 n'$, also $1 < n' < n$. Dann führt jede Primzerlegung $n' = p_2 \cdots p_s$ zu einer Primzerlegung $n = p_1 p_2 \cdots p_s$.

Dieser Beweis liefert zugleich ein bestimmtes Verfahren zur Gewinnung einer Darstellung (4): Man spaltet vom übrigbleibenden Faktor n' wieder den kleinsten Primteiler p_2 ab ($n' = p_2 n''$) und so weiter, bis nur noch ein Primfaktor übrigbleibt. So erhält man eine bestimmte Zerlegung $n = p_1 p_2 \cdots p_s$, in der $p_1 \leqq p_2 \leqq \cdots \leqq p_s$ ist. Hätte nämlich in einer Teilzerlegung $n = p_1 p_2 \cdots p_e f$ der Restfaktor f einen Primteiler $p < p_e$, so wäre auch $p \mid p_e f$ und somit p_e nicht der kleinste Teiler von $p_e f$. Man braucht also zur Fortsetzung der Zerlegung $f = p_{e+1} \cdots p_s$ nur Primzahlen $p \geqq p_e$ daraufhin zu prüfen, ob sie in f aufgehn, anderseits auch nur solche, deren Quadrat f nicht übersteigt; denn soll noch $f = ph$ zerlegbar sein, und ist $p^2 > f$, so $h^2 < f$. — Diese Zerlegung nach aufsteigenden Faktoren besagt aber noch nicht die Eindeutigkeit der Zerlegbarkeit (3) überhaupt.

Wir bringen jetzt den Eindeutigkeitsbeweis von Zermelo: Angenommen, die Primzerlegung sei nicht für alle n eindeutig. Dann müßte es wieder eine kleinste Zahl m dieser Eigenschaft geben, die also wenigstens zwei verschiedene Zerlegungen besäße. Dieses m besitzt genau eine Zerlegung (näm-

lich die durch die obige Methode gelieferte), in der sein kleinster Teiler q vorkommt; denn ist $m = qk$, so ist $k < m$ bereits eindeutig zerlegbar. Hat man eine zweite Zerlegung mit dem Primteiler p, und ist $m = pl$, so bilde man jetzt

$$m' = m - ql = (p - q)\,l. \tag{5}$$

Diese wegen $p > q$ positive Zahl $m' < m$ muß noch eindeutig zerlegbar sein. Nun ist

$$q \mid m' = q(k - l), \quad \text{wegen } m = qk,$$

müßte also in der Zerlegung der rechten Seite von (5) vorkommen, also, da l nur Primfaktoren $> q$ besitzt, in der Zerlegung von $p - q$. Aus $p - q = qr$ folgte aber $p = q(r + 1)$, und p wäre keine Primzahl. — Also kann auch m nur eine Zerlegung haben.

Der Fundamentalsatz gibt uns sofort Aufschluß über sämtliche Teiler einer Zahl n, wenn wir ihre Primzahlpotenzzerlegung (4) kennen: es ist jede Zahl

$$m = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r} \quad \text{mit} \quad 0 \leqq c_i \leqq a_i \tag{6}$$

Teiler von n, und umgekehrt hat jeder Teiler t von n diese Gestalt; denn einmal nach dem Eindeutigkeitssatz gehen keine andern Primzahlen in n auf als $p_1, \cdots p_r$, und es darf auch nicht etwa $c_1 > a_1$ sein; denn dann wäre

$$p_1^{a_1+1} \mid t \mid n = p_1^{a_1+1} v; \quad p_2^{a_2} \cdots p_r^{a_r} = p_1 v,$$

was nicht geht. Die Anzahl aller Teiler von n, einschließlich 1 und n, ist daher

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_r + 1), \tag{7}$$

das Produkt der Werteanzahlen, die jedes c_i unabhängig von den andern durchläuft (vgl. die Bemerkung zu 9. in § 3).

§ 5. Division mit Rest.

Es sei $m \geqq 0$ und $n \geqq 1$. Dann läßt sich eine „Division mit Rest" von m durch n auf die folgende Weise ausführen: Es gibt eine größte Zahl q, für die $nq \leqq m$ ist; denn es ist bereits $n(m + 1) > m$, anderseits $n \cdot 0 \leqq m$. Die x, die die Gleichung $nx \leqq m$ lösen, bilden daher einen echten Abschnitt der natürlichen Zahlenreihe, und der besitzt ein größtes Ele-

ment q. Es ist $q = 0$, wenn $m < n$, sonst positiv. Setzt man nun $m = nq + r$, so nennt man diese durch m und n gegebene Darstellung eine Division mit Rest. Dabei ist nach Definition von q der „Rest" $r = m - nq \geqq 0$, und zwar $= 0$ genau dann, wenn $n \mid m$. Anderseits ist $r < n$; denn sonst wäre noch $n(q+1) \leqq m$, gegen Voraussetzung. Zusammenfassend haben wir gewonnen:

Satz 10: Es gibt zu je zwei Zahlen $m \geqq 0$ und $n \geqq 1$ genau eine Darstellung

$$m = nq + r \quad \text{mit} \quad 0 \leqq r < n. \tag{8}$$

Dabei ist $q = 0$ kennzeichnend für $m < n$ und $r = 0$ für $n \mid m$. Den Quotienten q bezeichnen wir auch mit $\left[\frac{m}{n}\right]$, genannt: das „Ganze von m durch n", zum Unterschied von dem für $r > 0$ (hier nicht vorkommenden) gebrochenen Quotienten $\frac{m}{n}$. Für $r = 0$ darf die Klammer fortbleiben. Ebenfalls in einer Ungleichung $\frac{m}{n} < t$ oder $\frac{m}{n} \geqq t$ bei ganzem t.

Oft schreiben wir $m : n$ statt $\frac{m}{n}$.

Für die ganzen Quotienten bestätigt man sofort folgende Rechenregeln:

$$\left[\frac{[m:n]}{s}\right] = \left[\frac{m}{ns}\right], \tag{9}$$

$$\left[\frac{m_1 + m_2}{n}\right] = \left[\frac{m_1}{n}\right] + \left[\frac{m_2}{n}\right] + 0 \text{ oder } 1,$$

je nachdem in den Darstellungen $m_1 = nq_1 + r_1$ und $m_2 = nq_2 + r_2$ die Summe $r_1 + r_2 < n$ oder $\geqq n$ ausfällt. Ist insbesondere $r_1 = r_2 = 0$, also $n \mid m_1, m_2$, so auch $n \mid m_1 + m_2$. (Man stelle dieselbe Betrachtung für Differenzen an!)

Erste Formel (9) folgt so: Sind $m = nq + r$; $q = sv + w$ Divisionen mit Rest, so gibt v die linke Seite von (9). Es wird dann $m = n(sv + w) + r = nsv + nw + r$ eine Division durch ns mit dem Quotienten v und dem Rest $nw + r < nw + n = n(w+1) \leqq ns$. Also steht auch rechts v.

Die Division mit Rest ist ein wichtiges Hilfsmittel für zahlentheoretische Rechnungen und Beweise. Auf sie stützt

sich folgender neue Beweis von G. Klappauf für die Eindeutigkeit der Primfaktorzerlegung:

Entweder ist jede Zahl aus N eindeutig zerlegbar, oder es gibt eine kleinste Zahl m mit einer Doppelzerlegung

$$m = p_1 \cdots p_s = q_1 \cdots q_t.$$

Jedes p muß hier von jedem q verschieden sein; denn wäre etwa $p_1 = q_1$, so besäße bereits $\frac{m}{p_1}$ zwei verschiedene Zerlegungen. Sei nun q_1 die kleinste der Primzahlen p_1 bis q_t, so führe man für alle p_1 bis p_s die Division mit q_1 aus und erhält so für ihr Produkt m eine Darstellung

$$m = (q_1 Q_1 + R_1)(q_1 Q_2 + R_2) \ldots (q_1 Q_s + R_s) = q_1 Q + R,$$

indem nach wiederholter Anwendung des Distributivgesetzes bis auf das letzte Glied $R = R_1 \ldots R_s$ alle Glieder zu $q_1 Q$ zusammengefaßt werden. Weil $q_1 < p_1, \ldots p_s$ und Nichtteiler aller p, sind $Q_1, \ldots Q_s$, $R_1, \ldots R_s$ alle positiv, und daher gilt $0 < R < m$. Nun ist $q_1 \mid R$, hingegen $R = R_1 \ldots R_s$ eine Zerlegung in Faktoren $< q_1$, deren Primzerlegung also q_1 nicht aufweist! Dies widerspricht der Annahme, daß ein kleineres $R < m$ eine eindeutige Zerlegung besitzt.

Der hier gegebene Beweis braucht zwar schon mehr Hilfsmittel als der Zermelosche, der mit einer Subtraktion und Abspaltung je eines Primfaktors zweier m-Zerlegungen auskommt, gibt aber mit dem größeren Reduktionsschritt von m auf R einen weiteren Einblick in zahlentheoretische Verhältnisse. Für einen Induktionsbeweis leistet jedoch ein kleiner Schritt dasselbe.

II. Teilbarkeitseigenschaften.

§ 6. Der Ring der ganzen Zahlen. Moduln. Vielfachsummen.

Kommen wir im folgenden zwar weithin mit den natürlichen Zahlen aus, so ist es doch zur Vereinfachung von Rechnungen und für die Ausdrucksweise vorteilhaft, auch die negativen ganzen Zahlen zur Verfügung zu haben, schon um Summen und Differenzen nicht unterscheiden zu brauchen. Im wesentlichen werden wir aber bei den natürlichen Zahlen bleiben.

Wir führen den „Ring" der ganzen rationalen Zahlen als eine solche Erweiterung $\overline{Z}$ des natürlichen Zahlbereichs Z ein, in der eine entsprechend erweitert definierte Addition und Multiplikation sowie die Subtraktion als Umkehrung der Addition unbeschränkt ausführbar sind. Und zwar verfahren wir so:

Wir ergänzen den natürlichen Ordnungstypus zu einem symmetrischen

$$\ldots, -4, -3, -2, -1, \pm 0, +1, +2, +3, +4, \ldots$$

indem wir ein getreues Abbild $+0, +1, \ldots, +n, \ldots$ der natürlichen Zahlen, für das $+n$ die n-te auf $+0$ folgende Zahl ist, mit einem umgekehrten Abbild $\ldots, -n, \ldots -1, -0$, bei dem $-n$ die n-te der -0 vorangehende Zahl ist, unter Übereinstimmung von -0 mit $+0$ koppeln. Dies ergibt, soll eine geordnete Menge herauskommen, die einzige Anordnungsmöglichkeit

$$(10) \qquad -n < -m < -0 = +0 < +m < +n \quad \text{für} \quad 0 < m < n.$$

Diese so geordnete Zahlenreihe besitzt folgende kennzeichnende Eigenschaften:

$\overline{B}$. Jedes Element hat ein unmittelbar folgendes und ein unmittelbar vorangehendes Element (A. geht verloren.)

$\overline{C}$. Jeder echte Abschnitt besitzt ein letztes, jeder echte Rest ein erstes Element. (Rest = Menge der Art V auf S. 8 u.)

Man nennt jetzt ein $a > 0$ positiv, ein $a < 0$ negativ und bezeichnet als Absolutwert $|a|$ von a die natürliche Zahl n, für die $a = +n$ oder $-n$ ist; also den Abstand der Zahl a von 0. Durch Gleichsetzung von $+n$ mit n ordnet man Z als Teil in $\overline{Z}$ ein.

Die Rechenoperationen führen wir in $\overline{Z}$ so ein: Addition: Wie in Z sei $a + 0 = a$ und $a + m$ für $m > 0$ die m-te auf a folgende Zahl, während $a + (-m)$ die m-te Zahl vor a sei, die nach $\overline{C}$. immer existiert. Subtraktion: $c - a$ sei die nach $\overline{B}$., $\overline{C}$. immer existierende und eindeutige Lösung x der Gleichung $a + x = c$. Man setzt $0 - a = -a$. Es ist dann $c - a = c + (-a)$. Multiplikation mit positiven Zahlen sei wie in Z als wiederholte Addition definiert, $a \cdot 0 = 0$, $a \cdot (-1) = -a$, $a \cdot (-n) = (-a) \cdot n$. Dies ist dann gleichzeitig $-(a \cdot n)$, und allgemein ist

$$(-a)\cdot c = a\cdot(-c) = -ac, \quad (-a)\cdot(-c) = +ac.$$

Sind a und $c \neq 0$, so auch $ac = \pm |a|\cdot|c|$.

Die Rechenregeln 1.—9. aus § 2 erfahren in $\bar{Z}$ folgende Abänderungen: Entgegen 2. existiert die Differenz $n - m$, wie gesagt, auch für $n < m$; bei 7. (Vergleichbarkeit der Produkte) behält man $l \geqq 0$, $m > 0$ als Bedingung, aber keine Vorzeichenbedingung für r und n. Sonst bleiben alle Regeln erhalten. — Potenzierung wird als wiederholte Multiplikation nur mit natürlichen Exponenten verwandt.

Unter Restdivision eines a durch ein $m > 0$ wird neben der Darstellung mit „kleinstem positiven Rest"

$$a = m\cdot\left[\frac{a}{m}\right] + r, \quad 0 \leqq r < m$$

auch die Darstellung mit „kleinstem Absolutrest"

$$a = mv + w, \quad \frac{-m}{2} \underset{(=)}{<} w \leqq \frac{m}{2} \tag{11}$$

verstanden, z. B. $8 = 6\cdot 1 + 2$, $9 = 6\cdot 1 + 3$, $10 = 6\cdot 2 - 2$.

Durch wiederholte Division mit kleinstem Absolutrest gewinnt man (8) entsprechend eine Entwicklung nach Potenzen von m

$$a = m^k a_k + \cdots + m^i a_i + m^{i-1} a_{i-1} + \cdots + m\cdot a_1 + a_0, \tag{12}$$

wo $|a - m^k a_k| \leqq \frac{1}{2} m^k$, allgemein $r_i = m^{i-1} a_{i-1} + \cdots + a_0$ selbst absolut kleinster Rest nach m^i, wenn für $m = 2n$ auch $-n$ als Koeffizient a_{i-1} zugelassen und da anstatt n genommen wird, wo der Rest nach m^{i-1} positiv ist. Beispiel: $108 = 6^2\cdot 3$; $109 = 6^3 - 6^2\cdot 3 + 1$.

Als besonderes Ergebnis liefert die wiederholte Restdivision

Satz 11: Eine Summe von Zahlen, die alle bis auf eine durch m^k teilbar sind, ist nicht durch m^k, sondern nur durch die Potenz m^i, die in dieser einen Zahl aufgeht, teilbar.

Ist also $m^k \mid x_1 + \cdots + x_s$, ohne daß $m^k \mid x_1$, so gibt es wenigstens zwei Summanden, die nur durch die in allen Summanden aufgehende Potenz von m teilbar sind.

Wir bezeichneten den Bereich der ganzen rationalen Zahlen als „Ring", weil in ihm die Addition, Subtraktion und Multiplikation unter Gültigkeit der Rechenregeln 1., 4., 5, 6. uneingeschränkt ausführbar sind und die Produkte ac je zweier Zahlen wieder alle Zahlen

des Bereichs liefern, nämlich schon für $c = 1$.[1]) (Der Bereich „reproduziert sich durch Multiplikation". Für die Addition folgt das schon aus der vorhandenen Subtraktion). Die Kommutativität der Multiplikation zählt man gewöhnlich nicht zu den allgemeinen Ringeigenschaften, sondern spricht dann von einem „kommutativen Ring", ferner von einem „Ring ohne Nullteiler", wenn $ac = 0$ bei $a, c \neq 0$ im Ring nicht vorkommt. Ein kommutativer Ring ohne Nullteiler heißt auch „Integritätsbereich".

Ist im Ring schließlich wie in $\bar{Z}$ eine Ordnungsbeziehung eingeführt, und gelten die Vergleichbarkeitsregeln 3., 7., so spricht man von einem „geordneten Ring". $\bar{Z}$ ist also ein „geordneter Integritätsbereich".

Zwei weitere wichtige Begriffe sind „Modul" und „Vielfachsumme".

Modul heißt ein Bereich mit assoziativer und kommutativer Addition und unbeschränkter Subtraktion. Ein Modul ganzer rationaler Zahlen ist danach eine Teilmenge von $\bar{Z}$, der mit zwei Zahlen a, c auch $a + c$ und $a - c$ angehören. Das ist im allgemeinen noch kein Ring; es gilt hier

Satz 12: Jeder Modul ganzer rationaler Zahlen, der eine von 0 verschiedene Zahl enthält, besteht aus den Vielfachen einer einzigen Zahl m, der kleinsten positiven, die in ihm liegt.

Beweis: Liegt $a \neq 0$ in M, so auch $0 - a = -a$ und wegen wiederholbarer Addition alle ganzzahligen Vielfachen von a, von denen der eine Teil positiv ist. Also gibt es eine kleinste positive Zahl m in M. Nun dividiere man

$$a = mv + r \quad \text{mit} \quad 0 \leqq r < m.$$

Dann liegt mit a, m auch mv und $a - mv = r$ in M. Also kann wegen $r < m$ nicht $r > 0$ sein, da m die kleinste positive Zahl in M, und es ist $r = 0$, d. h. $a = mv$ selbst ein Vielfaches von m, wie Satz 12 behauptet.

Da auch umgekehrt die Vielfachen einer Zahl m immer einen Modul $(m) = (-m)$ bilden, sind somit alle Moduln ganzer rationaler Zahlen festgestellt.

[1]) Für die Definition des allgemeinen Ringes ist es sinngemäß, das Vorhandensein einer Eins e, die $ae = a$ für alle a erfüllt, zu fordern; vgl. W. Krull, Elementare Algebra, Sammlung Göschen, Bd. 930. Reproduktive Multiplikation gewährleistet noch keine Eins.

Da ferner die Produkte je zweier Zahlen aus (m) durch m^2 teilbar sind, ist die Multiplikation nur für $(m) = (1)$, d. h. $M = \bar{Z}$, und $(m) = (0)$ reproduktiv.

Vielfachsummen. Eine Zahl a heißt Vielfachsumme der Zahlen $a_1, a_2, \ldots a_n$, wenn sie sich in der Form

$$a = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = \Sigma a_i x_i \tag{13}$$

mit ganzen $x_1, \ldots x_n$ darstellen läßt oder, was hier dasselbe ist, als Differenz von Summen der a_i.

Satz 13: Die Gesamtheit $((a_1, \ldots a_n))$ der Vielfachsummen der a_i bilden einen Modul, fallen also nach Satz 12 mit den Vielfachen der kleinsten in der Form (13) darstellbaren Zahl s zusammen.

Jeder gemeinsame Teiler der Zahlen $a_1, \ldots a_n$ geht in jeder ihrer Vielfachsummen auf.

Beweis: Mit $\Sigma a_i x_i$ und $\Sigma a_i y_i$ ist auch $\Sigma a_i x_i \pm \Sigma a_i y_i = \Sigma a_i (x_i \pm y_i)$ Vielfachsumme. Und ist $t \mid a_i = t c_i$, so ist $\Sigma a_i x_i = t \cdot \Sigma c_i x_i$.

Umgekehrt ist ein gemeinsamer Teiler aller $\Sigma a_i x_i$ auch Teiler aller a_i; nämlich die a_i sind selbst Vielfachsummen

$$a_i = \Sigma a_j e_{ij} \quad \text{mit} \quad e_{ij} = 0 \quad \text{für} \quad i \neq j, \quad e_{ii} = 1. \tag{14}$$

Bemerkung: Ist eine unendliche Folge $a_1, \ldots, a_n, \ldots$ gegeben, so sind die Vielfachsummen der a_n natürlich Summen und Differenzen nur je endlich vieler dieser a_n. Eine einzelne Vielfachsumme läßt sich also in der Form

$$v = a_1 x_1 + \cdots + a_r x_r$$

mit einem von v abhängigen r schreiben. Summe und Differenz zweier Vielfachsummen sind wieder Vielfachsummen; alle v bilden darum einen Modul und sind Vielfache der kleinsten Vielfachsumme

$$s = a_1 z_1 + \cdots + a_m z_m, \tag{15}$$

also auch Vielfachsummen einer vom einzelnen v unabhängigen endlichen Teilmenge $a_1, \ldots, a_m$ der a_n.

Aufgaben: Man zeige, daß der Ordnungstypus von $\bar{Z}$ durch die Axiome $\bar{B}.$, $\bar{C}.$ bestimmt ist, d. h. daß je zwei geordnete Modelle $\bar{Z}', \bar{Z}''$, die $\bar{B}.$, $\bar{C}.$ erfüllen, unter Erhaltung der Ordnung aufeinander abbildbar sind. Man beachte: Die Abbildung zweier Modelle der natürlichen Zahlenreihe war eindeutig infolge Auszeichnung der Null als kleinstes Element. Hier aber sind alle Elemente in ihrer

Anordnung „gleichberechtigt“: es kann bei der Abbildung der Modelle $\overline{Z}'$ und $\overline{Z}''$ zuerst ein willkürliches Paar $(0', 0'')$ aus ihnen einander zugeordnet werden. Die Auszeichnung der Null und dann aller Zahlen geschieht bei Einführung der Addition.

Man versuche die Elemente aus $\overline{Z}$ konkret als Operationen, nämlich Additionen und Subtraktionen natürlicher Zahlen, zu deuten und diese wieder als ordnungsgetreue Abbildungen von $\overline{Z}$ auf sich. Was liefert dann die Multiplikation für Abbildungen?

Man beweise die bei Einführung der Rechenoperationen in $\overline{Z}$ aufgestellten Behauptungen und prüfe die Rechenregeln 1—9!

§ 7. Kleinstes gemeinsames Vielfaches. Größter gemeinsamer Teiler. Euklidischer Algorithmus.

Gegegeben seien die positiven Zahlen $a_1, a_2, \ldots a_n$. Ihr Produkt ist ein gemeinsames Vielfaches von $a_1, \ldots a_n$; sie besitzen daher ein (positives) kleinstes gemeinsames Vielfache $m = \{a_1, \ldots, a_n\}$. Von diesem gilt

Satz 14: Das kleinste gemeinsame Vielfache geht in allen gemeinsamen Vielfachen auf.

Beweis: Summe und Differenz gemeinsamer Vielfacher sind wieder gemeinsame Vielfache. Die gemeinsamen Vielfachen bilden also einen Modul, der nach Satz 12 aus den Vielfachen seiner kleinsten positiven Zahl besteht, also hier des kleinsten gem. Vielfachen von $a_1, \ldots a_n$.

Beispiel: $\{4, 6, 9\} = 36 \mid 4 \,.\, 6 \,.\, 9 = 36 \,.\, 6$.

Ferner betrachten wir die gemeinsamen Teiler der Zahlen $a_1, \ldots a_n$, deren kleinster 1 ist. Im Gegensatz zu den Vielfachen gibt es nur endlich viele gemeinsame Teiler; sie können z. B. a_1 nicht übertreffen. Infolgedessen gibt es hier einen größten gemeinsamen Teiler $d = (a_1, \ldots, a_n)$.

Satz 15 (vom größten gemeinsamen Teiler): Der größte gemeinsame Teiler $d = (a_1, \ldots, a_n)$ der Zahlen $a_1, \ldots a_n$ ist

A. durch alle gemeinsamen Teiler teilbar,

B. als Vielfachsumme von $a_1, \ldots a_n$ darstellbar:

$$d = a_1 x_1 + \cdots + a_n x_n. \tag{16}$$

Beweis: Nach Satz 13 und wegen (15) gilt

(17) $$t \mid s \mid a_1, \ldots, a_n$$

für jeden gemeinsamen Teiler t der a_i, wenn s die kleinste Vielfachsumme der a_i ist. Also ist dieses s, das die Eigenschaft B besitzt, selbst ein gemeinsamer Teiler mit der Eigenschaft A, also der größte: $s = d$ in (16).

Die Eigenschaft A sieht man als die wesentliche des gr. gem. T. an und führt ihn in Ringen ohne Ordnungsbeziehung auch so ein.

Ergänzende Definitionen: Auch für beliebige ganze Zahlen sollen $\{a_1, \ldots a_n\}$ und $(a_1, \ldots a_n, \ldots .)$ einen Sinn erhalten, und zwar soll $\{a_1, \ldots a_n\} = 0$ sein, wenn irgendein $a_i = 0$; denn dann ist 0 das einzige gemeinsame Vielfache; dagegen $(a_1, \ldots) = 0$ nur, wenn alle $a_i = 0$. Im übrigen werden als gemeinsame Teiler und Vielfache nur die positiven betrachtet und bleiben die Definitionen dieselben. Kl. gem. V. und gr. gem. T. sind dann immer natürliche Zahlen und ändern sich nicht, wenn man ein a_i durch $-a_i$ ersetzt.

Der gr. gem. T. behält, wie hier schon angedeutet, auch für unendlich viele a_i seinen Sinn; nach (15) sind dabei die a_i durch endlich viele aus ihnen ersetzbar, wegen Satz 15.

Weiter folgt aus den Definitionen und Satz 15: Notwendige und hinreichende Merkmale für $(a_1, \ldots a_n) = (c_1, \ldots c_m)$ sind einzeln

a) daß die gemeinsamen Teiler der a_i und c_i übereinstimmen,

b) daß $(a_1, \ldots a_n) \mid c_i$ und $(c_1, \ldots c_m) \mid a_i$,

c) daß die a_i und c_i dieselben Vielfachsummen haben. (Kriterien a) und b) auch für das kl. gem. V. bei Ersetzung der Teiler durch Vielfache.) — Ferner gelten die Regeln:

1. $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$.
$\{a_1, a_2, a_3\} = \{\{a_1, a_2\}, a_3\}$.

Die Wiederholung des Verfahrens läßt Zusammenfassungen $((a_1, \ldots a_m), \ldots, (a_r, \ldots, a_n))$ zu.

2. $(a_1, a_2, a_3, \ldots, a_n) =$
$(a_1, a_2 - a_1 y_2, a_3 - a_1 y_3, \ldots, a_n - a_1 y_n)$.

3. $(ca_1, ca_2, \ldots ca_n) = \mid c \mid \cdot (a_1, \ldots a_n)$.
$\{ca_1, \ldots ca_n\} = \mid c \mid \cdot \{a_1, \ldots a_n\}$.

4. $(a_0, a_1, \ldots a_n) \mid (a_1, \ldots a_n)$,
dabei $= (a_1, \ldots a_n)$, wenn ein anderes $a_i \mid a_0$. Insbesondere $(a, 0) = a$; $(a, 1) = 1$.

$\{a_1, \ldots a_n\} \mid \{a_0, a_1, \ldots a_n\}$; Gleichheit, wenn $a_0 \mid a_1$. $\{a, 1\} = a$; $\{a, 0\} = 0$. Regel 3 liefert das Kriterium

d) Ein gemeinsamer Teiler $\partial \mid a_1, \ldots a_n$ mit $a_i = \partial a_i'$ ist genau dann der größte, wenn $(a_1', \ldots, a_n') = 1$.

Beweise (durchgeführt nur für den gr. gem. T.):

1. Es ist $d = (a_1, a_2, a_3, \ldots a_n)$ als Teiler von a_1 und a_2 auch Teiler von (a_1, a_2), außerdem von $a_3, \ldots$, also auch von $d' = ((a_1, a_2), a_3, \ldots a_n)$. Umgekehrt geht d' außer in $a_3, \ldots$ auch in den Vielfachen a_1, a_2 von (a_1, a_2) auf.

2. Die Vielfachsummen sind links und rechts dieselben. Ohne Verwendung von Kriterium c): Aus $t \mid a_1, a_i$ folgt $t \mid a_i - a_1 y_i$ und hieraus umgekehrt mit $t \mid a_1$ zusammen $t \mid a_i$.

3. Ist $(a_1, \ldots a_n) = d$, so gilt $cd \mid ca_1, \ldots ca_n$, also $(ca_1, \ldots ca_n) = |c| de$ nach Satz 15 A. Aus $cde \mid ca_i$ folgt aber $de \mid a_i$, also $e = 1$.

4. $(a_0, a_1, \ldots a_n)$ ist gem. T. von $a_1, \ldots a_n$; ist $a_1 \mid a_0$, so auch $(a_1, \ldots a_n) \mid a_0$, gleichzeitig von $a_1, \ldots a_n$ und daher von $(a_0, \ldots a_n)$.

Wir werden jetzt ein Verfahren kennenlernen, den gr. gem. T. von n Zahlen zu bestimmen; für $n = 2$ ist es der Euklidische „Algorithmus".

Ist a_1 die kleinste der (positiv genommenen) Zahlen $a_1, \ldots, a_n$, deren gr. gem. T. wir feststellen wollen, so dividiere man alle a_i durch a_1, am vorteilhaftesten mit kleinstem Absolutrest

$$a_i = a_1 q_i \pm r_i, \quad 0 \leqq 2r_i \leqq a_1.$$

Dann ist nach Rechenregel 2.

$$(a_1, a_2, \ldots a_n) = (a_1, r_2, \ldots r_n).$$

Hierbei sind $r_2, \ldots r_n < a_1$, und ist dabei etwa r_2 die kleinste positive dieser Zahlen — eine solche gibt es, wenn nicht $a_1 | a_2, \ldots a_n$; $d = a_1$ — so verfahre man jetzt mit $r_2, \ldots r_n, a_1$ wie vorher mit $a_1, a_2, \ldots a_n$, dividiere also alles durch r_2, lasse dabei aber die $r_i = 0$ wieder fort. Da die kleinste Klammerzahl bei jeder Division abnimmt und eine abnehmende

Folge natürlicher Zahlen nach dem Ende von § 2 endlich ist, so muß das Verfahren abbrechen und mit einem Klammerpaar $(d, dt_2, \ldots dt_k) = (d, 0, \ldots 0)$ enden.

Beispiele für $n = 2$.

$(91, 133)$

$133 = 91 \cdot 1 + 42$
$91 = 42 \cdot 2 + 7$
$42 = 7 \cdot 6$

$(133, 91) = (91, 42) = (42, 7) = 7.$

Euklidischer Algorithmus.

$(89, 144)$

$144 = 89 \cdot 2 - 34$
$89 = 34 \cdot 3 - 13$
$34 = 13 \cdot 3 - 5$
$13 = 5 \cdot 3 - 2$
$5 = 2 \cdot 2 + 1$
$2 = 1 \cdot 2.$

$(144, 89) = (89, 34) = (34, 13) = (13, 5) = (5, 2) = (2, 1) = 1.$

Ein Beispiel für $n = 3$: $(481, 629, 663) = (481, 148, 182) = (148, 34, 37) = (37, 3, 0) = 1$. Anders: $(481, 629, 663) = (629, 34, 148) = (34, 17, 14) = (17, 3, 0) = 1$.

Wie die Durchführung der Rechnung zeigt, ist es bisweilen einfacher, statt des kleinsten bleibenden Restes einen solchen als Divisor für die nächste Division zu nehmen, der in der Nähe eines anderen Restes liegt. Auch wird man häufig die Rechenregel 1. der paarweisen Bildung des gr. gem. T. verwenden, insbesondere wenn sich von einem Paar (a_1, a_2) aus $(a_1, a_2, \ldots a_n)$ sofort der gr. gem. T. feststellen läßt. Ist dieser gar 1, so auch $(a_1, \ldots a_n)$. Bei unübersichtlich großen Zahlen bringt jedoch die simultane Division durch eine Klammerzahl die Reste schneller auf niedrige Zahlen.

Der Algorithmus gibt auch ein Verfahren, den gr. gem. T. als Vielfachsumme darzustellen: Hat man

$$(18) \qquad (a_1, a_2, \ldots a_n) = (a_1, r_2, \ldots r_n) = \cdots = d; \qquad a_i = a_1 q_i + r_i$$

und bereits eine Darstellung

$$(19) \qquad d = a_1 y_1 + r_2 y_2 + \cdots + r_n y_n$$

gewonnen, so gilt gleichzeitig

$$(20) \qquad d = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$$

mit $x_1 = y_1 - q_2 y_2 - \cdots - q_n y_n$, $x_2, \ldots x_n = y_2, \ldots y_n$.

Als Beispiel nehmen wir das obige für $n = 3$. Es ist

$$1 = 37 \cdot 1 - 3 \cdot 12 = 148 \cdot 0 + 34 \cdot 12 - 37 \cdot 11 = 148 \cdot 21 + 182 \cdot 12 - 481 \cdot 11 = 629 \cdot 21 + 663 \cdot 12 - 481 \cdot 44.$$

Bemerkung: Im Gegensatz zu den oben ausgeführten Algorithmen müssen in (19) die Reste r_i immer mit dem Vorzeichen behaftet sein, das sie bei der Division in (18) erhalten; nur dann stimmt (20) mit $x_2 = y_2, \ldots$. Ferner ist für $(a_1, \ldots a_n) = d \neq 1$, $a_i = da_i'$, die Lösung der Aufgabe (20) gleichwertig mit der Lösung der einfacheren Aufgabe:

$$1 = a_1' x_1 + \cdots + a_n' x_n.$$

$x_1 + ka_2'$, $x_2 - ka_1'$ ergeben für $n = 2$ aus einer Lösung (20) bei beliebig ganzem k alle Lösungen von (20). Auch für $n > 2$ gibt es unendlich viele Lösungen.

Zwischen dem kl. gem. V. und dem gr. gem. T. bestehen folgende Beziehungen: Es gilt Rechenregel

5. Für $(a_1, a_2) = d$, $\{a_1, a_2\} = m$ gilt $a_1 a_2 = md$. Insbesondere $\{a_1, a_2\} = m$ für teilerfremde a_1, a_2. — Allgemeiner:

Satz 16: Für $A = a_1 q_1 = a_2 q_2 = \cdots = a_n q_n$ gilt

$$A = \{a_1, \ldots a_n\}\,(q_1, \ldots q_n) = (a_1, \ldots a_n)\,\{q_1, \ldots q_n\}.$$

Beweis: Ist v ein in A aufgehendes gem. Vielfaches der a_i, so folgt aus $A = vw = a_i q_i$ und $a_i \mid v$, daß $w \mid q_i$, also ein gem. Teiler der q_i. Zu jedem v der Eigenschaft $v \mid A$ gehört dabei ein $w = A : v$ und zwar zum kleinsten $v_0 = \{a_1, \ldots a_n\}$ das größte w_0. (Das wegen $v_0 \mid v$ durch alle w teilbar ist.) Nun ist aber $d = (q_1, \ldots q_n)$ selbst ein w; denn ist $A = d\,e = a_i q_i$, so folgt aus $d \mid q_i$, daß $a_i \mid e$. Also ist $d = w_0$.

Dieser Beweis läßt gleichzeitig Satz 15 A über den gr. gem. T. als eine Folge des Satzes 14 über das kl. gem. V. erscheinen. Für $A = a_1 a_2 \cdots a_n$ und $n = 2$ erhält man Rechenregel 5. Für $A = a_1 a_2 a_3$ lautet z. B. die entsprechende Regel

$$a_1 a_2 a_3 = \{a_1, a_2, a_3\}\,(a_2 a_3, a_1 a_3, a_1 a_2).$$

Aufgaben: Man untersuche für $d = (a_1, a_2, a_3)$ die Lösungen von $d = a_1 z_1 + a_2 z_2 + a_3 z_3$.

Man zeige, daß im Euklidischen Algorithmus

$$(a_1, a_2) = (a_1, r) = (r, s)$$

für $a_1 < a_2$, sofern $a_1, a_2, r \neq 0$ ausfällt und man bei der Division immer den kleinsten Absolutrest wählt, bereits $s \leqq \frac{a_1}{5}$ wird, also

die kleinere Klammerzahl nach dem zweiten Schritt höchstens noch den fünften Teil der ursprünglichen ergibt.

Für $(a_1, a_2, a_3) = (a_1, r_1, r_2) = (r_1, s_1, s_2)$ ist, falls keine Division aufgeht, sogar s_1 oder $s_2 \leqq \frac{a_1}{7}$.

§ 8. Teilerfremdheit. Klassischer Beweis des Fundamentalsatzes.

Wenn zwei Zahlen a und c keinen andern gemeinsamen Teiler als 1 besitzen, wenn also $(a, c) = 1$ ist, nennt man a und c „teilerfremd", „relativ prim" oder „prim" zueinander und schreibt auch $a \smile c$. Auch n Zahlen $a_1, \ldots a_n$ heißen teilerfremd, wenn $(a_1, \ldots a_n) = 1$, dagegen „paarweis teilerfremd", wenn je zwei der Zahlen $a_1, \ldots a_n$ teilerfremd sind, was schon für $n = 3$ mehr bedeutet: im letzten Algorithmusbeispiel ist weder $481 \smile 629$ noch $629 \smile 663$ noch $481 \smile 663$, aber $(481, 629, 663) = 1$. Ein Kriterium für paarweise Teilerfremdheit liefert Satz 20; wir kehren zur bloßen Teilerfremdheit zurück und beweisen

Satz 17 (der Teilerfremdheit): Ist $(a, b) = (a, c) = 1$, so auch $(a, bc) = 1$.

Beweis (durch wiederholte Anwendung von Satz 15 A): Es ist $(a, bc) \mid ac, bc$; also $(a, bc) \mid (ac, bc) = (a, b) \cdot c = c$. Da zugleich $(a, bc) \mid a$, ist $(a, bc) \mid (a, c) = 1$.

Folgerung 1: $(a_1 a_2 \cdots a_m, c_1 \cdots c_n) = 1$, wenn $(a_i, c_k) = 1$ für jedes Paar i, k.

Wie wiederholte Anwendung von Satz 17 liefert.

Folgerung 2: Aus $(a, b) = 1$; $a \mid bc$ folgt $a \mid c$. Weil dann zugleich $a \mid (ac, bc) = (a, b)\, c$.

Wir wenden diese Ergebnisse auf Primzahlen und ihre Potenzen an. Da eine Primzahl p nur die Teiler 1 und p hat, ist

$$(p, a) = 1 \quad \text{oder} \quad p,$$

d. h. eine Zahl a ist zu einer Primzahl entweder teilerfremd oder durch sie teilbar. Für zwei verschiedene Primzahlen gilt dann

$$(p, q) = 1.$$

Infolgedessen liefert Satz 17 für eine Primzahl $p = a$:

Hauptsatz 18: Geht die Primzahl p weder in m noch in n auf, so geht sie auch im Produkt mn nicht auf. Positiv: Geht eine Primzahl p in einem Produkt mn auf, so geht sie wenigstens in einem der Faktoren m, n auf.

Wiederholte Anwendung ergibt: Potenzen p^r und q^s verschiedener Primzahlen sind teilerfremd. Ferner:

Satz 19: Geht ein Primzahlpotenzprodukt $p_1^{a_1} \cdots p_r^{a_r}$ mit positiven Exponenten a_i in einem andern $q_1^{c_1} q_2^{c_2} \cdots q_s^{c_s}$ auf, so kommen alle Primfaktoren des linken Produkts auch als Faktoren des rechten Produkts vor, und zwar mit demselben oder einem höheren Exponenten.

Kommt nämlich p_1 unter den q_2 bis q_s nicht vor, so ist $(p_1^{a_1}, q_2^{c_2} \cdots q_s^{c_s}) = 1$, also $p_1^{a_1} \mid q_1^{c_1}$ wegen $p_1^{a_1} \mid q_1^{c_1} \cdots q_s^{c_s}$.

Dieses Ergebnis enthält aber den Fundamentalsatz.

Schließlich liefert Satz 17 das Kriterium für paarweise Teilerfremdheit von $a_1, a_2, \ldots a_n$:

$$(21)\quad (a_1 a_2 \cdots a_{n-1},\ a_1 \cdots a_{n-2} a_n,\ \ldots,\ a_2 a_3 \cdots a_n) = 1.$$

In der Klammer stehn alle Produkte von je $n-1$ der Zahlen a_i. Dies Kriterium ergibt nach Satz 16 der

Satz 20: $\{a_1, a_2, \ldots a_n\} = a_1 a_2 \cdots a_n$ gilt genau dann, wenn $a_1, a_2, \ldots a_n$ paarweis teilerfremd.

Beweis: Paarweise Teilerfremdheit ist jedenfalls notwendig; denn ist etwa $(a_1, a_2) = d \neq 1$, so ist bereits $\frac{a_1 a_2}{d} a_3 \cdots a_n$ ein Vielfaches der $a_1, \ldots a_n$. Daß sie auch hinreichend ist, besagt für $n = 2$ Regel 5. des § 7 und folgt induktiv so: Ist für je $n-1$ paarweis teilerfremde Zahlen das kl. gem. V. gleich dem Produkt, so ist bei paarweis teilerfremden $a_1, \ldots a_n$ das Produkt $a_2 \cdots a_n = \{a_2, \ldots a_n\} \mid \{a_1, a_2, \ldots a_n\}$, aber auch $a_1 \mid \{a_1, \ldots a_n\}$ und daher $\{a_1, a_2 \cdots a_n\} \mid \{a_1, a_2, \ldots a_n\}$, anderseits $\{a_1, a_2 \cdots a_n\} = a_1 \cdot a_2 \cdots a_n$, weil mit $(a_1, a_2) = \cdots = (a_1, a_n) = 1$ nach Satz 17 auch $(a_1, a_2 \cdots a_n) = 1$ gilt. Hiermit ist Satz 20 bewiesen.

Nach dem Satz über den gr. gem. T. gibt es dann für jede Zerlegung $A = a_1 a_2 \cdots a_n$ der Zahl A in paarweis teilerfremde Faktoren a_i eine Darstellung

$$1 = \frac{A}{a_1} x_1 + \frac{A}{a_2} x_2 + \cdots + \frac{A}{a_n} x_n - Ay, \tag{22}$$

der im Bereich der rationalen Zahlen die Partialbruchzerlegung

$$\frac{1}{A} = \frac{x_1}{a_1} + \frac{x_2}{a_2} + \cdots + \frac{x_n}{a_n} - y \tag{23}$$

entspricht. Legt man x_i auf $0 \leqq x_i < a_i$ oder $-a_i < 2x \leqq a_i$ fest, so sind $x_1, \ldots x_n, y$ eindeutig.

§ 9. Primzahlverteilung.

Ein sehr altes und immer noch brauchbares Verfahren, eine Primzahltafel von 2 bis zu einer gegebenen Zahl n aufzustellen, ist das „Sieb des Eratosthenes“:

Es werden die Zahlen von 2 bis n aufgeschrieben, 2 bleibt als Primzahl stehn und alle höheren geraden Zahlen werden als zusammengesetzt gestrichen; sodann bleibt von den ungeraden Zahlen 3 als Primzahl stehn, und alle höheren Vielfachen $3m$ von 3 sind wieder zu streichen. Allgemein geht das Verfahren so: sind durch die Aussiebung $2, 3, 5, \ldots p$ als Primzahlen festgestellt und die höheren Vielfachen dieser Primzahlen gestrichen, so ist die erste auf p folgende stehngebliebene Zahl q die nächste Primzahl, da sie durch keine der Primzahlen $2, 3, \ldots p$ teilbar ist; zu streichen sind nun wieder alle noch dastehenden höheren Vielfachen von q, das sind aber die $qm \leqq n$ mit $m > 1$ und $(m, 2 \cdot 3 \cdots p) = 1$, als erste q^2; denn geht eine der Primzahlen bis p in m auf, so wurde qm schon früher gestrichen. Das Verfahren braucht daher nur solange fortgesetzt zu werden, bis ein r mit $r^2 > n$ als Primzahl stehn bleibt.

Wir wollen hier eine Tafel der Primzahlen bis 300 aufstellen und nehmen an, die Aussiebung sei schon für die Vielfachen von 2, 3, 5 durchgeführt. Wir brauchen dann nur 2, 3, 5 und die höheren zu 30 teilerfremden Zahlen aufzuschreiben:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 49 53 59
61 67 71 73 77 79 83 89 91 97 101 103 107 109 113 119
121 127 131 133 137 139 143 149 151 157 161 163 167 169 173 179
181 187 191 193 197 199 203 209 211 217 221 223 227 229 233 239
241 247 251 253 257 259 263 269 271 277 281 283 287 289 293 299

Zuerst fallen die unterstrichenen Zahlen 7.7, 7.11, 7.13, fort, dann die mit zwei, drei und vier Punkten versehenen Vielfachen von 11, 13, 17. Die übrigen sind Primzahlen. Vgl. weiter Kap. VI. § 35.

Die periodische Wiederkehr der zu $2 \cdot 3 \cdots p$ teilerfremden Zahlen kann in der Primzahlreihe keine Periodizität zur Folge haben, da bei ihrer Fortsetzung immer neue Streichungen vorzunehmen sind; schon die erste Periode der zu $2 \cdot 3 \cdot 5 \cdot 7 = 210$ Teilerfremden weist mehrere zusammengesetzte (oben punktierte) Zahlen auf. Es besitzt überhaupt jede „arithmetische Progression"

$$r,\ r+m,\ r+2m,\ r+3m, \ldots \tag{24}$$

zusammengesetzte Zahlen, z. B. $r + 2rm + rm^2 = r(m+1)^2$. Umgekehrt besagt der berühmte Dirichletsche Satz über die arithmetische Progression, daß jede „teilerfremde Progression" (24), d. h. in der $(r, m) = 1$ gilt, unendlich viele Primzahlen enthält. Dieser Satz ist bisher als Ganzes nur mit höheren Mitteln bewiesen worden; jedoch lassen sich Teile dieses Satzes (Satz 49) auf arithmetischem Wege ähnlich dem Euklidischen Satze von der unendlichen Anzahl der Primzahlen überhaupt beweisen. Der Dirichletsche Satz liefert sogar eine gewisse Gleichverteilung der Primzahlen auf die verschiedenen teilerfremden Progressionen einer Differenz m.

Über die Häufigkeit der Primzahlen kann man aus dem Siebverfahren entnehmen, daß sie allmählich seltener werden, wenn auch in recht unregelmäßiger Folge und sehr langsam. Immerhin wird die Primzahlfolge beliebig dünn; aber man muß in einer Primzahltabelle von n aus schon bis etwa n^2 weiterblättern, um die Primzahldichte auf die Hälfte herabzubringen. Während man z. B. in einer Tafel der Quadrate schon bei $4n$ dasselbe erreicht. (Analytischer Maßstab: die

Summe $\sum \frac{1}{p}$ der reziproken Primzahlen divergiert, was Euler zum Nachweis der Existenz unendlich vieler Primzahlen verwandte; die Reziprokensumme der Quadratzahlen aber konvergiert.) Das prägnanteste Ergebnis über die Verteilung der Primzahlen ist der von Gauß schon vermutete und Hadamard und de la Vallée-Poussin bewiesene Primzahlsatz, daß das Verhältnis der Anzahl $\pi(n)$ der Primzahlen bis n und der Funktion $n : \log n$ (oder das Verhältnis der n-ten Primzahl p_n zu $n \cdot \log n$) mit wachsendem n gegen 1 geht.

Kann man auf diese Weise Aussagen über die Häufigkeit der Primzahlen im großen ganzen machen, so sind im einzelnen ihre Abstände sehr unregelmäßig. Aus dem Primzahlsatz kann man zwar entnehmen und in einzelnen Teilen einfacher beweisen, daß von gewissem n an das Verhältnis zweier aufeinanderfolgender Primzahlen enger als ein vorgegebenes $h : h+1$ ist, aber in der Differenz tauchen an einigen Stellen plötzlich für die ganze Umgebung ungewöhnlich hohe Lücken auf. So liegt z. B. zwischen 1327 und 1361 keine Primzahl; diese Lücke wird zum erstenmal wieder durch das Primzahlpaar 8467, 8501 erreicht und durch 9551, 9587 überboten. Anderseits sind „Primzahlzwillinge“ q, $q+2$ weithin recht häufig (sogar Primzahlvierlinge gibt es zwischen 290000 und 300000 noch: 294311, 13, 17, 19; 295871, 73, 77, 79; 299471, 73, 77, 79). Ob es unendlich viele gibt, weiß man noch nicht; ihre Reziprokensumme ist nach Viggo Brun konvergent.

Aufgabe: Man zeige, daß es in einem Hundert aufeinanderfolgender Zahlen höchstens 23 zu $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$ prime Zahlen gibt, daß es daher in einem Hundert oberhalb 17 höchstens 23 Primzahlen geben kann, wie tatsächlich von 18 bis 117!

Daß es umgekehrt primzahlfreie Hunderte gibt, wird aus § 15 folgen, ebenfalls, daß es unter den Hunderten mit zu $2 \cdot 3 \cdot 5 \ldots 17$ primen 23 Zahlen auch solche gibt, wo die 23 Zahlen zu allen Primzahlen bis zu einer Zahl p prim sind.

Merkwürdige Unregelmäßigkeiten in der Primzahlfolge finden sich auch in einzelnen arithmetischen Progressionen. So ist in der Kraitchikschen Tafel der Primzahlen von der Form $2^9 k + 1$ die

erste $7681 = 512 \cdot 15 + 1$, während eine Differenz der Mindestgröße $512 \cdot 15$ erst wieder nach der 37. Primzahl der Tabelle auftritt.

Ein besonderes Interesse haben die Mersenneschen Primzahlen der Form $2^m - 1$ und die (Fermat-) Gaußschen der Form $2^m + 1$ gewonnen. Allgemeiner gefragt: Welche algebraischen Teiler von $x^n - 1$ sind für $x = 2$ Primzahlen?

$2^m - 1$ kann nur für eine Primzahl $m = p$ wieder Primzahl sein; denn für $m = pm'$ mit $m > 1$ ist $2^p - 1$ echter Teiler von $2^m - 1$, und $m = 1$ ergibt 1. Es liefern

(25) $\quad p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$

wirklich Primzahlen $2^p - 1$. Dagegen gilt $23 \mid 2^{11} - 1$, $47 \mid 2^{23} - 1$, $167 \mid 2^{83} - 1$ (vgl. § 27); $223 \mid 2^{37} - 1$, $233 \mid 2^{29} - 1$, $431 \mid 2^{43} - 1$. Für die übrigen $p < 100$ ist $2^p - 1$ auch zusammengesetzt.

Von größerem Interesse, nämlich für die Frage der Kreisteilung mit Hilfe von Zirkel und Lineal, sind die Gaußschen Primzahlen der Form $2^m + 1$. Hier muß m selbst eine Zweierpotenz sein: $m = 2^s$. Denn für $m = 2^s \cdot u$ mit ungeradem $u > 1$ gilt $2^{2^s} + 1 \mid 2^m + 1$. Man kennt nur fünf Primzahlen dieser Gestalt, nämlich

(26)
$$\begin{array}{lllll} p = & 3, & 5, & 17, & 257, \quad 65537 \\ m = & 1, & 2, & 4, & 8, \quad 16 \\ s = & 0, & 1, & 2, & 3, \quad 4. \end{array}$$

Während (entgegen einer Behauptung von Fermat, alle $2^{2^s} + 1$ seien Primzahlen) bereits für $s = 5$

(27) $\quad 5 \cdot 2^7 + 1 = 641 \mid 2^{32} + 1$ (vgl. § 27)

und auch $s = 6, 7, 8, 9, 11, 12$ zusammengesetzte Zahlen (Kraitchik II, 221) liefern.

Nach Gauß gelingt die t-Teilung des Kreises mit Zirkel und Lineal für ungerades t nur, wenn t ein quadratfreies Produkt Gaußscher Primzahlen (kombinierbar durch Partialbruchzerlegung, z. B. die 255-Teilung durch Halbierung der Differenz des fünfzehnten und siebzehnten Kreisteils). Die maximal bisher mögliche Ungeradteilung ist die in $3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 = 2^{32} - 1$ gleiche Teile.

Allgemein kann man von den Fermatschen Zahlen $F_s = 2^{2^s} + 1$ wenigstens sagen, daß sie unendlich viele Primteiler besitzen;

denn alle Primteiler der $F_s (s < r)$ gehen in deren Produkt $2^{2^r} - 1 = F_r - 2$ auf, also nicht in F_r, und daher muß die Primzerlegung von F_r aus lauter neuen Faktoren bestehn.

Eine andere Folge mit immer neuen Primteilern ist

$$c_i = c_1 c_2 \ldots c_{i-1} + 1 \quad \text{mit} \quad c_1 = 2.$$

Es werden $c_2 = 3$, $c_3 = 7$, $c_4 = 43$, $c_5 = 1807 = 13 \cdot 139$. Schließlich zeigen wir:

Satz 21: Jedes ganzzahlige Polynom

$$A(x) = a_n x^n + \cdots + a_1 x + a_0 \quad (a_n > 0,\ n > 0)$$

besitzt unendlich viele Primteiler.

Eine Primzahl heißt dabei Primteiler von $A(x)$, wenn $p \mid A(a)$ für irgend ganzzahlige a. Und zwar weist die Folge

$$y_0 = A(x_0),\quad y_1 = A(x_1), \ldots, y_s = A(x_s), \ldots$$

immer neue Primteiler auf bei einer Argumentewahl

$$x_0 > 2 \mid a_i \mid,\quad x_1 = x_0 + y_0^2,\quad \text{allgemein}\quad x_{s+1} = x_s + y_s^2.$$

Beweis: Dadurch, daß x_0 das Doppelte der Koeffizienten-Absolutwerte von $A(x)$ übertrifft, stellt $A(x_0)$ eine Entwicklung (12) nach x_0 dar, und es gilt daher

$$A(x_0) > a_n x_0^n - \frac{x_0^n}{2} \geqq \frac{x_0^n}{2} > 1.$$

Also besitzt $y_0 = A(x_0)$ wenigstens einen Primteiler, und dieser geht in $y_1 = A(x_0 + y_0^2) = A(x_0) + y_0^2 B(x_0, y_0)$ in gleicher Potenz wie in y_0 auf, weil $y_0 \mid y_1$, aber $(y_1, y_0^2) = y_0$; für $y_1 = y_0 q_1$ ist also $(q_1, y_0) = 1$. Daher kann sich q_1 nur aus Nichtteilern von y_0 zusammensetzen, liefert also wirklich neue Primteiler für $A(x)$, wenn $q_1 > 1$. Und dies ist der Fall wegen

$$x_1 = x_0 + y_0^2 > 2 \mid a_i \mid,\quad y_1 > a_n \left[\frac{x_1^n}{2}\right] > \left[\frac{y_0^{2n}}{2}\right] > y_0.$$

Ebenso gilt allgemein $y_s = y_{s-1} q_s$ mit $(q_s, y_{s-1}) = 1$ und $q_s > 1$. Jedesmal kommt also wenigstens ein neuer Primteiler hinzu. Obendrein hat man gewonnen:

Die Wertfolge $A(0), A(1), \ldots A(n), \ldots$ eines Polynoms A kann nicht nur aus Primzahlen bestehn, sondern stellt auch zusammengesetzte Werte dar. Eine besonders lange Primzahlfolge ($-39 \leqq x \leqq 40$) hat das Polynom $A(x) = x^2 - x + 41$.

§ 10. Zahlentheoretische, summatorische, distributive Funktion.

Zahlentheoretische Funktion heißt eine Funktion $f(n)$, die jeder positiven ganzen Zahl n wieder einen ganzzahligen Funktionswert zuordnet oder allgemeiner einen Funktionswert $f(n)$ aus irgendeinem die ganzen Zahlen umfassenden Ring, z. B. eine reelle Zahl. Im Bedarfsfall wird $f(0) = 0$ hinzugenommen.

Jedes Polynom stellt z. B. für seine ganzen positiven Argumente eine zahlentheoretische Funktion im Ring der ganzen Zahlen dar. In der Regel denkt man aber an Anzahlfunktionen, von denen wir in (7) schon kennenlernten die Funktion $\tau(n) =$ Anzahl der Teiler von n. Ihr Bildungsprinzip erzeugt einen neuen zahlentheoretischen Begriff:

Summatorische Funktion $F(n) = Sf(n)$ von $f(n)$ heißt die Funktion

$$F(n) = \sum_{d \mid n} f(d). \tag{28}$$

Die Summierung wird also über alle und nur die Argumente erstreckt, die Teiler von n sind, einschließlich 1 und n.

Aus den Potenzen entstehen so die *Teilerfunktionen*

$$\sigma_k(n) = \sum_{d \mid n} d^k.$$

Dabei ist $\sigma_0(n) = \tau(n)$ unsere Teileranzahl und $\sigma_1(n) = \sigma(n)$ die ebensohäufig vorkommende Summe der Teiler von n.

Diese sowie andere wichtige zahlentheoretische Funktionen haben die Eigenschaft der „Distributivität“:

Distributive Funktion heißt eine zahlentheoretische Funktion, wenn

$$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2) \quad \text{für} \quad (n_1, n_2) = 1 \tag{29}$$

gilt, für $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ also

$$f(n) = f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdot \dots \cdot f(p_r^{a_r}). \tag{30}$$

Insbesondere $f(1) = 1$, wenn man die Funktion $f(n) = 0$ nicht als distributiv zählt. Gilt außerdem $f(p^a) = f(p)^a$ und somit $f(n_1 n_2) = f(n_1) \cdot f(n_2)$ für jedes Paar (n_1, n_2), so heißt f eine multiplikative Funktion. $\tau(n)$ ist nach (7) z. B. distributiv, aber nicht multiplikativ. Es gilt nun der

Satz 22: Die summatorische Funktion einer distributiven Funktion ist wieder distributiv.

Beweis: Sei $f(n)$ distributiv und $n_1 \smile n_2$, so wird

$$(31) \qquad \sum_{\substack{d \mid n \\ (n=n_1 n_2)}} f(d) = \sum_{\substack{d_1 \mid n_1 \\ d_2 \mid n_2}} f(d_1 \cdot d_2) = \sum_{d_1 \mid n_1} f(d_1) \cdot \sum_{d_2 \mid n_2} f(d_2).$$

Dabei gewinnt man die $F(n_1) \cdot F(n_2)$ ergebende Produktdarstellung rechts in (31) mit Hilfe des distributiven Rechengesetzes aus dem mittleren Ausdruck und diesen aus dem linken so: die Produkte $d_1 d_2$ durchlaufen sicher alle Teiler von n, und zwar für $n_1 \smile n_2$ auch nur einmal; denn bei $n = p_1^{a_1} \dots p_s^{a_s}$ und passender Anordnung der Primfaktoren p_i wird dann $n_1 = p_1^{a_1} \dots p_r^{a_r}$ mit $r < s$, und $d_1, d_2, d_1 d_2$ haben alle Exponentenkombinationen c_1 bis c_r, c_{r+1} bis c_s, c_1 bis c_s mit $0 \leqq c_i \leqq a_i$ zu durchlaufen.

Da die Potenzen n^a gewiß distributive Funktionen sind, so auch als ihre Summatorfunktionen die Teilerfunktionen, die sich daraufhin leicht berechnen lassen:

$$\sigma_r(p^a) = 1 + p^r + p^{2r} + \dots + p^{ar} = \frac{p^{r(a+1)} - 1}{p^r - 1}$$

und dann $\sigma_r(\Pi p^a) = \Pi \sigma_r(p^a)$. Insbesondere

$$(32) \qquad \sigma(n) = \prod_{p_i \mid n} \frac{p_i^{a_i+1} - 1}{p_i - 1} \quad \text{für } n = \Pi p_i^{a_i}.$$

Ein frühes Interesse haben die „vollkommenen" Zahlen, die gleich der Summe ihrer übrigen Teiler sind, gewonnen, also der Fall $\sigma(n) = 2n$. Vollkommene Zahlen sind nach (32) jedenfalls die $2^{p-1}(2^p - 1)$, wo $2^p - 1$ Primzahl. Ist umgekehrt $n = 2^{s-1} \cdot u$ eine gerade vollkommene Zahl ($s > 1$, u ungerade), so muß

$$2^s u = \sigma(2^{s-1} u) = (2^s - 1) \cdot \sigma(u)$$

sein, also $2^s - 1 \mid u$, weil prim zu 2^s. Bei $u = (2^s - 1)\, q$ ergibt das: $\sigma(u) = 2^s q = q + u$. Danach sind q und u die einzigen Teiler von u und dann $q = 1$ und $u = 2^s - 1$ Primzahl. — Für ungerade vollkommene Zahlen sind nur stark einschränkende Bedingungen bekannt, nichts aber über ihre Existenz.

Bemerkenswert ist noch die Beziehung

$$\sum_{a=1}^{n} \tau(a) = \sum_{m \geqq 1} \left[\frac{n}{m}\right]. \tag{33}$$

(Links nicht summatorische Funktion von τ, sondern von 1 bis n durchsummiert!)

Bezeichnet nämlich $h(n)$ die rechte Summe, deren Summierung wegen $\left[\frac{n}{m}\right] = 0$ für $m > n$ nach oben nicht begrenzt zu werden braucht, so gilt $\left[\frac{n}{m}\right] - \left[\frac{n-1}{m}\right] = 1$ für $m \mid n$, sonst 0, also $h(n) - h(n-1) = \tau(n)$.

§ 11. Die Möbiussche und die Eulersche Funktion.

Wir behandeln jetzt die umgekehrte Aufgabe, aus einer Summatorfunktion $F(n) = \sum_{d \mid n} f(d)$ die ursprüngliche Funktion $f(n)$ zu ermitteln. Wir beweisen zuerst

Satz 23: Zu jeder zahlentheoretischen Funktion $F(n)$ gibt es genau eine Funktion $f(n)$, deren Summatorfunktion sie ist. Ist $F(n)$ distributiv, so auch $f(n)$ und dann

$$f(n) = \prod_{p} (F(p^a) - F(p^{a-1})) \text{ für } n = \prod p^a. \tag{34}$$

Induktionsbeweis: Es sei richtig, daß es genau eine für die Zahlen $m < n$ definierbare Funktion $f(m)$ mit der Eigenschaft $\sum_{l \mid m} f(l) = F(m)$ gibt.

Dann gibt es genau eine Fortsetzung $f(1), \ldots f(n-1), f(n)$, für die auch $\sum_{d \mid n} f(d) = F(n)$ wird; denn man braucht nur

$$f(n) = F(n) - \Sigma f(d), \quad d \text{ echter Teiler von } n,$$

zu definieren, und dies ist, nachdem $f(1)$ bis $f(n-1)$ festliegen, die einzige Möglichkeit, um (28) zu erfüllen.

Daß mit $F(n)$ auch $f(n)$ distributiv ist, folgt nun zugleich mit (34) so: Es ist jedenfalls $f(p^a) = F(p^a) - F(p^{a-1})$ wegen

$$F(p^a) = f(1) + f(p) + \cdots + f(p^{a-1}) + f(p^a).$$

Man definiere jetzt eine distributive Funktion

$$h(n) = \prod_p (F(p^a) - F(p^{a-1})),\ n = \prod p^a,$$

die für $n = p^a$ mit $f(n)$ übereinstimmt. Ihre Summatorfunktion $H(n)$ ist nach Satz 22 ebenfalls distributiv, und es ist durch Definition $H(p^a) = F(p^a)$. Beides zusammen ergibt $H(n) = F(n)$, also $f(n) = h(n)$.

Für die distributiven Funktionen ist damit die Aufgabe, $f(n)$ aus $F(n)$ zu bestimmen, gelöst. Wir suchen nun allgemein einen geschlossenen Ausdruck, der $f(n)$ als Vielfachsumme der $F(m)$, $m \mid n$, darstellt:

$$(35)\quad f(n) = \mu_1 F(n) + \cdots + \mu_t F\left(\frac{n}{t}\right) + \cdots + \mu_d F\left(\frac{n}{d}\right) + \cdots + \mu_n F(1).$$

Die Argumente seien nach fallenden Teilern von n geordnet.

Es wird sich zeigen, daß $\mu_d = \mu(d)$ nur von d, nicht aber von n und F abhängt: Jedenfalls muß schon $\mu_1 = 1$ sein, da $f(n)$ bei summatorischer Zerlegung der $F(t)$ nach (28) nur in $F(n)$ vorkommt. Die übrigen $f(d)$ müssen hingegen nach Einsetzen von (28) aus der Darstellung (35) herausfallen. Dabei kommt $f\left(\frac{n}{d}\right)$ zum letztenmal bei $F\left(\frac{n}{d}\right)$ als Summand vor und vorher bei allen $F\left(\frac{n}{t}\right)$, wo t echter Teiler von d. Hat man daher alle μ_t $(t < d)$ schon so bestimmt, daß $f\left(\frac{n}{t}\right)$ für $1 < t < d$ aus der Teilsumme $\mu_1 F(n) + \cdots + \mu_t F\left(\frac{n}{t}\right)$ von (35) und damit ganz aus (35) herausfällt, so braucht man jetzt nur μ_d als negative Summe aller μ_t mit echtem Teiler t von d anzusetzen, und es fällt auch $f\left(\frac{n}{d}\right)$ heraus.

Nach diesem Ansatz hängt $\mu(d)$ tatsächlich nur von d ab, und man hat eine Darstellung (35), kennt man nur die *Möbiussche Funktion* $\mu(d)$. Für sie gilt nach (35):

$$(36)\qquad \sum_{d \mid n} \mu(d) = o(n) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & ,, \ n > 1. \end{cases}$$

Ihre summatorische Funktion $o(n)$ ist also distributiv und daher nach Satz 23 auch $\mu(n)$. Nach (34) liefert (36):

$$\mu(1)=1,\ \mu(p)=-1,\quad \mu(p^2)=\mu(p^3)=\cdots=0.$$

(37) $\mu(n)=(-1)^r$ für quadratfreies $n=p_1\cdots p_r$,
$\mu(n)=0$ für quadratbehaftetes n.

Zusammenfassend haben wir gewonnen:

Satz 24 (Möbiussche Umkehrungsformel): Ist $F(n)$ die summatorische Funktion von $f(n)$, so ist $f(n)$ rückwärts aus F bestimmbar durch die Formel

$$f(n)=\sum_{d\mid n}\mu(d)\,F\left(\frac{n}{d}\right). \tag{38}$$

Hierbei ist $\mu(n)$ die durch (37) angegebene Funktion.

Wir wenden diese Ergebnisse auf die *Eulersche Funktion* $\varphi(n)$, die Anzahl der zu n teilerfremden Zahlen von 1 bis n (0 bis $n-1$), an, eine Funktion von Bedeutung für das nächste Kapitel. Wir stellen fest, daß

$$\sum_{m\mid n}\varphi(m)=n. \tag{39}$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

Beweis von (39): Man ordne die Zahlen r von 1 bis n nach ihrem gr. gem. T. d mit n. Aus $(r,n)=d$ mit $r=dq$, $n=dm$ folgt $(q,m)=1$ und umgekehrt. Ebenfalls bedingt sich $0<r\leqq n$ und $0<q\leqq m$ gegenseitig, und daher ist $\varphi(m)$ als Anzahl der zu m teilerfremden Zahlen von 1 bis m zugleich die Anzahl der Zahlen von 1 bis n, die mit n den gr. gem. T. $d=n:m$ haben. Geht man alle $d\mid n$ durch, so wird damit die Anzahl n aller Reste die Summe der $\varphi(m)$ mit $m\mid n$. Man hat

Satz 25: Die Eulersche Funktion $\varphi(n)$ hat n als Summatorfunktion, ist daher distributiv, und es ist $\varphi(p^a)=p^a-p^{a-1}$, nach (34) für $n=\Pi\,p^a$ also

$$\varphi(n)=\prod_{p\mid n}(p^a-p^{a-1})=\prod_{p\mid n}(p-1)\,p^{a-1} \tag{40}$$
$$=n\prod_{p\mid n}\frac{p-1}{p}\quad\text{in Bruchform geschrieben.}$$

Die Möbiussche Formel (38) liefert sodann

$$\varphi(n) = \sum \mu(d) \frac{n}{d}. \tag{41}$$

Eine Verallgemeinerung des eben Gewonnenen ist folgende Aufgabe: Man bilde die n^k Systeme $a_1, \ldots, a_k$ der unabhängig voneinander die Zahlen von 0 bis $n-1$ durchlaufenden a_i und verteile sie nach dem gr. gem. T. $d = (a_1, \ldots a_k, n)$ in Klassen. Die Anzahl der Systeme mit $d = 1$ heiße $\varphi_k(n)$. Es gilt dann entsprechend

$$\sum_{m \mid n} \varphi_k(m) = n; \quad \varphi_k(m) = \sum \mu(d) \frac{n^k}{d^k}.$$

Wir stellen die gewonnenen distributiven Funktionen in einem Schema zusammen, in dem jeweils die rechts von einer Funktion stehende deren summatorische ist:

$$\begin{array}{l} \mu, o, 1, \tau; \\ \varphi, n, \sigma; \end{array} \quad \varphi_k, n^k, \sigma_k.$$

III. Kongruenzen.

§ 12. Rechnen mit Kongruenzen. Der Restklassenring.

Die Restdivision $a = mv + r$ durch eine positive Zahl m teilt alle ganzen rationalen Zahlen nach dem Rest r in m Restklassen $\bar{r} = \bar{0}, \bar{1}, \ldots m-\bar{1}$ ein. Wie wir sehen werden, hängt die Restklasse einer Summe und eines Produktes von Zahlen nur von den Restklassen dieser Zahlen ab. Dies wird die Bildung eines „Restklassenringes modulo m“ ermöglichen, in dem außerdem die Multiplikation in weiterem Maße umkehrbar ist als im Ring der ganzen Zahlen. Die Kongruenzen, die wir gleich definieren werden, sind im wesentlichen nichts anderes als Gleichungen zwischen Restklassen, nur daß eine Kongruenz eine Beziehung zwischen einzelnen Zahlen aus den Restklassen darstellt, zwischen „Resten“, indem man zwei Zahlen als „kongruent“ erklärt, wenn sie derselben Restklasse angehören.

Wir werden indes den Begriff der Kongruenz lieber etwas anders einführen, nämlich so, daß er in allen Teilbarkeitsbe-

reichen auch ohne eine bestimmte Division mit Rest anwendbar ist. Wir definieren nun:

(42) $\qquad a' \equiv a \bmod m$ bedeute $m \mid a' - a$.

Gesprochen: a' kongruent a modulo m; oft kürzer geschrieben: $a' \equiv a\,(m)$ oder nur $a' \equiv a$, wenn der *Modul* m bekannt ist. Die Bezeichnung Modul entspricht unserer früheren Definition des Moduls insofern, als $z \equiv 0\,(m)$ genau für die Zahlen z des Moduls (m) gilt.

Die Kongruenz ist eine Äquivalenzbeziehung, d. h. es gilt

Symmetrie $\quad a \equiv a'$ mit $a' \equiv a$

Transitivität und $\quad a'' \equiv a$ „ $a' \equiv a$ und $a'' \equiv a'$.

Denn es ist mit $m \mid a' - a$ auch $m \mid a - a'$ und, wenn außerdem $m \mid a'' - a'$, auch $m \mid (a'' - a') + (a' - a) = a'' - a$. Ferner gilt $a \equiv a$ (Reflexivität, die aus Symmetrie und Transitivität auf dem Wege $a \equiv a' \equiv a$ folgt).

Jede Äquivalenzbeziehung liefert eine Einteilung in „Klassen untereinander äquivalenter Elemente“ (hier kongruenter Zahlen) derart, daß zwei Elemente verschiedener Klassen inäquivalent sind (hier inkongruent: $a \not\equiv b\,(m)$, wenn $m \nmid a - b$). Diese Klassen nennen wir hier Restklassen mod m und jeden Vertreter einer Klasse einen Rest.

Wie schon erwähnt, sind Addition (Subtraktion) und Multiplikation invariant gegen Kongruenzübergänge: Ist

$$a' \equiv a,\ b' \equiv b,\ c' \equiv c \bmod m,$$

so gilt

$$\begin{aligned} &a' \pm b' \equiv a \pm b \quad \text{wegen} \quad m \mid (a' - a) \pm (b' - b) \\ &\qquad\qquad\qquad\qquad\qquad\quad = (a' \pm b') - (a \pm b); \\ (43)\quad &a'c \equiv ac \qquad\quad \text{„} \qquad m \mid (a' - a)\,c = a'c - ac; \\ &a'c' \equiv a'c \equiv ac. \end{aligned}$$

Durch beliebige Verbindung der Ringoperationen erhält man für $x \equiv y,\ x_i \equiv y_i$ allgemein

$$\begin{aligned} &a_0 + a_1 x + \cdots + a_k x^k \equiv a_0 + a_1 y + \cdots + a_k y^k \\ (44)\quad \text{und} \qquad &A(x_1, \ldots x_n) \equiv A(y_1, \ldots, y_n). \end{aligned}$$

Hierbei bedeute A ein Polynom in mehreren Variabeln mit ganzen Koeffizienten, also $A(x_1, \ldots x_n)$ einen Ausdruck, der aus $x_1, \ldots x_n$ durch Additionen und Multiplikationen hervor-

geht. Der jedem System ganzer $x_1, \ldots x_n$ dabei zugeordnete Funktionswert $A(x_1, \ldots x_n)$ ist daher wieder nur von den Restklassen abhängig, in denen die x_i liegen. Auch dürfen die Koeffizienten durch kongruente Werte ersetzt werden, immer mod m. Nicht aber dürfen Exponenten von Potenzen mod m abgeändert werden (jedoch oft mod $\varphi(m)$; vgl. § 17), um wieder eine Kongruenz mod m zu erhalten.

Daß für Kongruenzen auch die Rechengesetze eines Ringes gelten, erhält man am besten durch Bildung des Restklassenringes mod m. Man definiert als Summe, Differenz, Produkt zweier Restklassen mod m diejenige Restklasse, die die Summe, Differenz, das Produkt je einer Zahl aus den beiden Restklassen enthält; sie ist nach (43) eindeutig bestimmt. So erhält man einen Restklassenring mod m, der die in § 6 gestellten Forderungen eines kommutativen Ringes erfüllt. Wir werden jedoch der Restklassengleichung die Kongruenz als einfachere Ausdrucksweise vorziehn.

Beispiele: $m = 5.\ \overline{3} \cdot \overline{3} = \overline{4} = -\overline{1}.$

$m = 9.\ \overline{3} \cdot \overline{1} = \overline{3} \cdot \overline{4} = \overline{3} \cdot \overline{7} = \overline{3}.$

$\overline{3} \cdot (\overline{4} - \overline{7}) = \overline{3} \cdot (-\overline{3}) = \overline{0}.$

Im Kongruenzen geschrieben:

$3 \cdot 3 \equiv 9 \equiv 4 \equiv -1 \bmod 5.$

$3 \,.\, 1 \equiv 3 \cdot 4 \equiv 3 \cdot 7 \equiv 3 \bmod 9\,. \ldots$

Das zweite Beispiel zeigt schon, daß der Ring mod 9 Nullteiler besitzt und daher keine eindeutig umkehrbare Multiplikation. Für zusammengesetztes $m = kl\ (k, l < m)$ hat der Ring mod m stets Nullteiler, nämlich die Restklassen $\overline{k}$ und $\overline{l}$; denn es gilt $kl \equiv 0 (m)$ bei $k, l \not\equiv 0$. Ist hingegen m Primzahl, so gibt es nach Hauptsatz 18 kein solches Paar k, l, und daher ist der Restklassenring eines Primzahlmoduls nullteilerfrei (vgl. § 13).

Der Umstand, daß der Restklassenring mod m eine endliche Menge ist, wird uns manche wertvolle Schlußweise liefern und macht es ferner möglich, vollständige Additions- und Multiplikationstabellen aufzustellen. Z. B.

0 1 2 3 4 5	1 2 3 4 5 0	1 2 3 4 5 6
1 2 3 4 5 0	2 4 0 2 4 0	2 4 6 1 3 5
2 3 4 5 0 1	3 0 3 0 3 0	3 6 2 5 1 4
3 4 5 0 1 2	4 2 0 4 2 0	4 1 5 2 6 3
4 5 0 1 2 3	5 4 3 2 1 0	5 3 1 6 4 2
5 0 1 2 3 4	0 0 0 0 0 0	6 5 4 3 2 1
Add. mod 6	Mult. mod 6	Mult. mod 7

Dabei steht das Produkt (die Summe) eines Restes r am linken Rande mit einem Rest s am oberen Rand in derselben Zeile wie r und Spalte wie s, und es ist die Multiplikation $0 \cdot r = r \cdot 0 = 0$ in der Tabelle mod 7 kürzehalber fortgelassen. Als Vertreter seiner Restklasse wurde jedesmal der kleinste positive Rest verwandt; es könnte auch irgendein Vertreter für jede Restklasse gewählt werden, mod 7 z. B. 1, 9, 3, 18, 12, −1, 7.

Ein solches System R, das aus jeder Restklasse mod m genau eine Zahl enthält, heißt ein *vollständiges Restsystem* mod m. Dieses ist durch je zwei der folgenden drei Eigenschaften bereits gekennzeichnet:

1. R enthält genau m Zahlen.
2. Je zwei Zahlen aus R sind einander inkongruent.
3. Jede ganze Zahl ist einer Zahl aus R kongruent.

Jede der drei Eigenschaften folgt aus den andern beiden, jeweils unter Verwendung des Anzahlsatzes (Satz 4).

Hat man ein bestimmtes vollständiges Restsystem R mod m festgelegt, so „reduziert" man eine Kongruenz, indem man in ihr jede Zahl durch die zu ihr kongruente aus R ersetzt.

Bemerkung 1. Der Restklassenring R_m mod m geht allein schon aus dem Begriff der natürlichen Zahl hervor: um die Restklasse $-\bar{1}$ zu definieren, braucht man die negativen Zahlen nicht einzuführen, denn die Gleichung $\bar{x} + \bar{1} = \bar{0}$ ist lösbar durch die Restklasse $\bar{x} = m - 1$; sie ist also keine Neueinführung. Ähnlich verhält es sich mit der Umkehrung der Multiplikation im nächsten Paragraphen.

Bemerkung 2. Den Ring der ganzen rationalen Zahlen kann man selbst als den „Restklassenring mod 0" auffassen, weil in ihm die Restklasse 0 aus der den Modul (0) erschöpfenden Zahl 0 allein besteht. Die Nullteilerfreiheit, die bei ihm schon aus der Ordnung seiner Elemente folgt, hat er mit den Primzahlmodul-Restklassenringen gemein. Bei diesen hat man aber wie bei allen eigentlichen Restklassenringen nur eine zyklische Anordnung seiner Elemente.

Übergang von einem Modul $m = dt$ zu einem Modulteiler t.

(45) Mit $a' \equiv a\,(m)$ gilt $a' \equiv a\,(t)$.
Mit $a' \equiv a\,(t)$ gilt $a'd \equiv ad\,(m)$ und umgekehrt.

Nämlich $t \mid a - a'$ ist gleichbedeutend mit $dt \mid da - da'$. Während $a' \equiv a \bmod m$, also $dt \mid a' - a$ mehr sagt.

§ 13. Kongruenzdivision. Bruchdarstellung. Restklassenkörper.

Satz 26: Die Kongruenz $ax \equiv c \bmod m$ ist genau dann lösbar, wenn $(a, m) \mid (c, m)$ und besitzt in diesem Fall gerade (a, m) einander inkongruente Lösungen. Für den Hauptfall $(a, m) = 1$ gehört also zu jedem c eine mod m eindeutige Kongruenzlösung.

Beweis: Nach Definition der Kongruenz bedeutet $ax \equiv c \bmod m$, daß sich ax von c nur um ein Vielfaches von m unterscheidet, also $ax = c + my$ für irgend ganzes y oder

$$c = ax - my. \tag{46}$$

Zu jeder Lösung der linearen Kongruenz $ax \equiv c\,(m)$ gehört somit ein Lösungspaar x, y der diophantischen Gleichung (46), und umgekehrt liefert das x eines Lösungspaares von (46) stets eine Lösung der linearen Kongruenz. Durch $ax - my$ sind aber gerade alle Vielfachen von (a, m) darstellbar. Also ist $(a, m) \mid c$ oder $(a, m) \mid (c, m)$ die notwendige und hinreichende Bedingung für die Lösbarkeit der Kongruenz $ax \equiv c\,(m)$.

Ist nun $(a, m) = d$, $a = a'd$, $c = c'd$, $m = m'd$, so ist $ax \equiv c\,(m)$ nach (45) gleichwertig mit $a'x \equiv c'\,(m')$, wie sich ja auch (46) auf $a'x - m'y = c'$ reduziert, und aus einer Lösung x erhält man alle durch $x' = x + m'z$ mit beliebig ganzem z (vgl. § 7); denn es ist $a'x' \equiv a'x\,(m')$ oder $m' \mid a'(x' - x)$ wegen $(a', m') = 1$ nur für $m' \mid x' - x$.

Ist von vornherein $(a, m) = 1$, so gilt $x' \equiv x\,(m)$; man hat in diesem Falle, wie behauptet, eine mod m eindeutige Lösung. Sonst sind, sofern $(a, m) \mid c$ gilt, x, $x + m'$, $x + 2m'$, ... $x + (d - 1)\,m'$ alle d einander mod m inkongruenten Lösungen; anders ausgedrückt: die Lösung ist eindeutig mod m'. Damit ist alles bewiesen.

Für $(a, m) = 1$ verwendet man zur Bezeichnung der eindeutigen Lösung der Kongruenz $ax \equiv c \bmod m$ gern die Bruchform $x \equiv \frac{c}{a} \bmod m$. Wir führen aber mit dieser Bruchschreibweise nicht die rationalen Zahlen ein, auch nicht die mit zu m fremdem Nenner. Das letzte ginge an sich, würde aber den Begriff der Kongruenz mod m sowie der Teilbarkeit überhaupt verschieben. Es gelten aber hier dieselben Rechenregeln wie für rationale Brüche:

$$(47) \qquad \frac{cs}{as} \equiv \frac{c}{a}; \quad \frac{c}{a} \cdot \frac{r}{s} \equiv \frac{cr}{as}; \quad \frac{c}{da} \pm \frac{r}{ds} \equiv \frac{cs \pm ar}{das}.$$

Die Bruchschreibweise kann die Auflösung von Kongruenzen sehr vereinfachen. Dies sei an zwei Beispielen dargetan:

$$27x \equiv 1 \ (100) : \ x \equiv \frac{1}{27} \equiv -\frac{99}{27} \equiv -\frac{11}{3} \equiv -\frac{111}{3} \equiv -37$$

oder

$$\equiv \frac{189}{3} \equiv 63.$$

$$67x \equiv 81 \ (139) : \ x \equiv \frac{81}{67} \equiv -\frac{81}{72} \equiv -\frac{9}{8} \equiv -\frac{148}{8} \equiv -\frac{37}{2} \equiv 51$$

oder

$$\equiv \frac{162}{134} \equiv -\frac{23}{5} \equiv \frac{116}{5} \equiv 51.$$

Das Prinzip ist folgendes: den Nenner des gegebenen Bruches dadurch allmählich auf 1 herabzudrücken, daß man Zähler wie Nenner durch kongruente Zahlen ersetzt, entweder kleinere oder aber so zerfallende, daß der Bruch nach (47) kürzbar wird. Bisweilen kann auch eine Brucherweiterung wie oben $\frac{81}{67} = \frac{162}{134}$ das Verfahren beschleunigen; der in Zähler und Nenner hinzukommende Faktor muß dabei aber zu m prim sein. In der Regel kommt man mit dem Bruchrechnungsverfahren viel schneller zum Ziel als durch Auflösung einer diophantischen Gleichung (46) nach dem Muster des Euklidischen Algorithmus. Umgekehrt lohnt es sich, wenn (46) gegeben, eine Bruchkongruenz daraus zu machen, wobei noch die Auswahl zwischen a und m als Modul steht.

Eine besondere Würdigung verdient der Fall, daß der Modul der Kongruenz eine Primzahl ist. Auf ihn werden sich

(§ 16) die Kongruenzen nach beliebigem Modul im wesentlichen zurückführen lassen. Es gilt hier

Satz 27: Der Restklassenring eines Primzahlmoduls ist ein Körper.

Körper heißt dabei ein kommutativer Ring, in dem jede Gleichung $ax = c$ für $a \neq 0$ eine, und zwar dann eindeutige, Lösung besitzt, die restlose Division $\frac{c}{a}$ also ausführbar ist.

Die Eindeutigkeit folgt hier aus der allgemeinen Existenz der Lösung: Gilt zugleich $ax = ay = c$, so $a(x-y) = 0$ bei $x - y \neq 0$. Es hat dann nach Festsetzung auch $(x-y)z = 1$ eine Lösung z, und es gilt $a = a(x-y)z = 0 \cdot z = 0$. Für $a \neq 0$ ist daher die Lösung eindeutig.

Umgekehrt kann man nur für Ringe mit endlich vielen Elementen schließen: Sind alle ax verschieden, wenn x den Ring durchläuft, so ergeben die ax nach Satz 4 alle Ringelemente. Es ist darum ein *nullteilerfreier endlicher Ring ein Körper*, also auch der in § 12 bereits als nullteilerfrei festgestellte R_p. Dagegen ist der unendliche Ring der ganzen Zahlen zwar nullteilerfrei, aber kein Körper.

Die Körpereigenschaft des Restklassenringes R_p mod p folgt jedoch unmittelbar aus Satz 26; denn $ax \equiv c$ ist mod p für jedes $a \not\equiv 0\,(p)$, d. h. jedes nicht durch p teilbare a lösbar, weil dann $(a, p) = 1$.

Die Lösung $x = a'$ von $ax \equiv 1\,(p)$ heißt der zu a *reziproke* Rest. Hat man eine Reziprokentafel mod p, so kann man Divisionen durch Multiplikationen ersetzen.

§ 14. Ein Satz von Thue. Wilsonscher Satz.

Wir bringen jetzt einige Anwendungen der Restdivision, zuerst in verallgemeinerter Form einen Satz von *Axel Thue*, der sowohl für zahlentheoretische Rechenverfahren (VI) als für abzählende Beweise (§ 20) wertvoll ist:

Satz 28: Sind e und f zwei natürliche Zahlen, deren Produkt die Primzahl p übersteigt, dabei $1 < e, f \leqq p$, so lassen sich alle Reste r mod p auf die Gestalt bringen:

$$(48) \quad r \equiv 0 \text{ oder } \pm\frac{x}{y} \text{ mit } 0 < x < e, \quad 0 < y < f.$$

(Bei Thue ist $f = e$ und e das Minimum, für das $e^2 > p$.)

Beweis mit Hilfe der Dirichletschen Schubfächermethode: Ist r ein fester Rest $\not\equiv 0 \bmod p$, so bilde man alle Ausdrücke $v + rw$ mit $0 \leqq v < e, 0 \leqq w < f$. Das sind ef, also mehr als p, Ausdrücke; also sind wenigstens zwei unter ihnen einander kongruent, etwa $v' + rw' \equiv v'' + rw''$ und dabei $w' \not\equiv w''$, weil sonst auch $v' \equiv v''$. Dann ist aber, wie zu zeigen war,

$$r \equiv \pm \frac{|v' - v''|}{|w' - w''|} \text{ mit } 0 < |v' - v''| < e, \quad 0 < |w' - w''| < f.$$

Die Unterbringung der Reste im Bruchrechteck $0 < x < e$, $0 < y < f$ liefert dabei selbst im quadratischen (Thueschen) Fall $e = f$ eine sehr ökonomische Verteilung: für $p = 3, 7, 23, 47$ hat man nur je eine Darstellung $\pm \frac{x}{y}$ mit $(x, y) = 1$ für die Reste $1, \ldots p - 1$.

Für sonstige p haben mehr als die Hälfte aller Reste auch nur eine Darstellung: der Überschuß an Darstellungsmöglichkeiten beträgt weniger als die halbe Restzahl. Für große p bleibt der Überschuß zwischen 21 und 22% [1,215 $< Q(n) : n^2 <$ 1,216 für großes n bei $Q(n) = 4 \sum_{m \geqq n} \varphi(m) - 1$ Darstellungen $0, \pm \frac{x}{y}$ für ein p zwischen n^2 und $(n+1)^2$.]

Nun eine Anwendung der Reziprokenbildung mod p:

Satz 29 (Wilsonscher Satz, bewiesen von Lagrange): Für jede Primzahl p gilt

$$(49) \quad (p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv -1 \bmod p;$$

$$(50) \quad \left(\frac{p-1}{2}\right)! \equiv j \text{ mit } j^2 \equiv -1 \,(p) \text{ für } p = 4n+1,$$

$$(51) \quad \equiv \pm 1 \,(p) \qquad \text{für } p = 4n-1.$$

Das wichtigste Ergebnis liegt hier in (50): daß die Kongruenz $x^2 \equiv -1 \,(p)$ lösbar ist für $p \equiv 1 \,(4)$. Wann in (51) $+1$ und wann -1 steht, vgl. S. 97/98.

Beweis von (49): Ist x' jeweils der reziproke Rest zu x, also $xx' \equiv 1 \,(p)$, so ordne man das Produkt (49) nach Paaren x, x' unter Voranstellung der Selbstreziproken $x' = x$, für die also $x^2 \equiv 1$ gilt, d. h. $p \mid x^2 - 1 = (x-1)(x+1)$ und dann

$p \mid x-1$ oder $x'+1$; $x \equiv \pm 1 (p)$. Es folgt

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

Beweis von (50), (51) für $p = 2k+1$ aus (49): Es ist $-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdots k(-k) \cdot\cdot\ (-2)(-1) = (-1)^k (k!)^2$. Für $p = 4n+1$ (k gerade) also $(k!)^2 \equiv -1$; $k! \equiv j$, für $p = 4n-1$ aber $(k!)^2 \equiv +1$; $k! \equiv \pm 1$.

§ 15. Simultane Kongruenzen.

Satz 30 (Hauptsatz über simultane Kongruenzen): Gegeben seien r paarweis teilerfremde Moduln $m_1, m_2, \ldots m_r$ mit dem Produkt m und zu jedem m_i ein Rest a_i. Dann gibt es mod m genau einen Rest x, der die Kongruenzen

(52) $\qquad x \equiv a_1 (m_1),\ x \equiv a_2 (m_2), \ldots\ x \equiv a_r (m_r)$

zugleich erfüllt, wie auch die a_i gewählt seien.

Die aus der Verbindung der Kongruenzen (52) hervorgehende Kongruenz mod m ist dabei gleichwertig mit (52), weil auch umgekehrt aus ihr alle Kongruenzen (52) folgen.

Folgerung: Eine Kongruenz nach einem zusammengesetzten Modul ist gleichwertig mit einer Schar von Kongruenzen nach seinen Primzahlpotenzfaktoren.

Beweis von Satz 30: Ist $m = m_i q_i$ und dann $(q_1, \ldots q_r) = 1$ wegen paarweiser Teilerfremdheit der m_i, so ist

$$1 = q_1 y_1 + \cdots + q_r y_r$$

darstellbar. Setzt man dabei $q_i y_i = z_i$, so hat man

(53) $\quad 1 = z_1 + z_2 + \cdots + z_r$ mit $\begin{matrix} z_j \equiv 0 (m_i) \\ z_i \equiv 1 (m_i) \end{matrix}$ für $j \neq i$.

Nämlich $m_i \mid q_j = m : m_j \mid z_j$ und daher $z_i \equiv 1 (m_i)$. Setzt man nun

(54) $\qquad x \equiv a_1 z_1 + a_2 z_2 + \cdots + a_r z_r \bmod m,$

so ist (52) erfüllt, und jede (52) erfüllende Zahl $x' \equiv x\ (m)$ hat, weil $x' - x$ durch alle m_i teilbar sein muß, denselben Rest mod m. (54) liefert mit (53) ein Rechenverfahren.

Beispiel: $x \equiv 2 \bmod 7$, $x \equiv 4 \bmod 8$, $x \equiv 1 \bmod 9$. Wird bei $(7, 8) = (7, 9) = (8, 9) = 1$ durch einen bestimmten Rest mod $7 \cdot 8 \cdot 9 = 504$ erfüllt. Es ist $q_1 = 72 \equiv 2\,(7)$; $q_2 = 63 \equiv -1\,(8)$; $q_3 = 56 \equiv 2\,(9)$. Für die Rechnung genügt es, (53) als Kongruenz mod m anzusetzen; man hat dann für y_i nur $q_i y_i \equiv 1\,(m_i)$ zu lösen, und hat $q_1 y_1 + \cdots + q_r y_r \equiv 1\,(m_i)$; hier also $2y_1 \equiv 1$; $y_1 \equiv 4 \bmod 7$, $y_2 \equiv -1 \bmod 8$, $y_3 \equiv -4 \bmod 9$. Diese y in (53) eingesetzt ergibt

$$z_1 \equiv 288,\ z_2 \equiv -63,\ z_3 \equiv -224\ (504).$$

Also $x = 2 \cdot 288 - 4 \cdot 63 - 224 \equiv 100 \bmod 504$.

Dies Verfahren ist vorteilhaft, wenn mehrere Kongruenzverbindungen nach denselben Moduln vorzunehmen sind. Soll z. B. jetzt $x \equiv 5\,(7)$, $x \equiv 1\,(8)$, $x \equiv 3\,(9)$ bestimmt werden, so erhält man mit denselben z jetzt

$$x \equiv -2 \cdot 4 \cdot 27 - 63 - 3 \cdot 4 \cdot 56 \equiv -72 - 63 + 6 \cdot 56 \equiv 201.$$

Hat man jedoch nur ein System simultaner Kongruenzen zu vereinigen, so ist es oft vorteilhafter, statt der Kongruenzen $q_i y_i \equiv 1$ gleich $q_i x_i \equiv a_i$ aufzulösen und dann $x = x_1 + \cdots + x_r$ zu bilden. Jedenfalls beachte man, daß der Multiplikand von q_i nur von seiner Restklasse mod m_i abhängt und daher mod m_i reduziert werden kann, wie im letzten Beispiel oben geschehn, auch unter Verwendung von Bruchdarstellungen, deren Nenner jedoch bei der Aufstellung von (54) zu m prim sein muß.

Anderes Rechenverfahren: Man vereinige die Kongruenzen (52) der Reihe nach so, daß man zuerst das erste Paar durch eine einzige Kongruenz mod $m_1 m_2$ ersetzt und x durch $x - a_1$:

$$x - a_1 \equiv 0\,(m_1);\ x - a_1 \equiv a_2 - a_1\,(m_2),$$

$$(55)\quad x - a_1 = m_1 y \equiv a_2 - a_1\,(m_2);\ y \equiv \frac{a_2 - a_1}{m_1} \bmod m_2.$$

y muß, etwa nach dem Bruchverfahren unter (47), ganzzahlig ausgedrückt werden und liefert dann ein $x \equiv a_{12} \bmod m_1 m_2$. Nun fahre man wie oben fort mit der Vereinigung von

$$x - a_{12} \equiv 0\,(m_1 m_2);\ x - a_{12} \equiv a_3 - a_{12}\,(m_3)$$

und gelangt zu $x \equiv a_{123}\,(m_1 m_2 m_3)$; $x \equiv a_4\,(m_4)$; $\ldots\ x \equiv a_r\,(m_r)$. Ausgeführt am zweiten obigen Beispiel $x \equiv 201\ (504)$:

$x - 5 = 7y \equiv 1 - 5 \bmod 8$; $y \equiv 4$, $x \equiv 5 + 7 \cdot 4 \equiv 33\,(56)$.
$x - 33 = 56\,z \equiv 3 - 6 \bmod 9$; $z = 3$, $x \equiv 33 + 168\,(504)$.

Dies i. allg. günstigere Verfahren gestattet auch,

(56) $\quad x \equiv a_1\,(m_1)$; $x \equiv a_2\,(m_2)$ bei $(m_1, m_2) = d$

als Aufgabe zu behandeln. Hier muß $a_1 \equiv a_2\ (m_1, m_2)$ sein, damit $(m_1, m_2) \mid x - a_1, x - a_2$, und dies reicht auch für die Lösbarkeit von (56); denn setzt man durchweg $n = dn'$ für $d \mid n$, so bleibt für y in (55) nur eine Kongruenz $m_1' y \equiv (a_2 - a_1)' \bmod m_2'$ zu lösen, und durch dies mod m_2' eindeutig bestimmte y ist auch $x = a_1 + m_1 y$ nach dem Modul $m_1 m_2' = \{m_1, m_2\}$ bestimmt. Das allgemeine Ergebnis lautet hier:

Satz 31: Die Kongruenzen (52) sind allgemein genau dann erfüllbar, wenn

(57) $\quad a_i \equiv a_k \bmod (m_i, m_k)$ für jedes Paar i, k

gilt, und dann ist x genau mod m, dem kl. gem. V. der m_i, bestimmt.

Beweis: Klar ist, daß (57) gelten muß, wenn eine Lösung x existieren soll, daß dann ferner x, weil nach allen m_i, auch mod m festliegen muß und mit x auch jedes $x + mq$ Lösung ist. Daß (57) auch hinreichend ist, folgt mit Induktionsschluß so: Satz 31 sei richtig für ein System von $r - 1$ simultanen Kongruenzen. Dann gibt es also für die ersten $r - 1$ Kongruenzen (52) ein gemeinsames

$$x \equiv a \mod m' = \{m_1, \ldots m_{r-1}\},$$

und es bleibt

$$x - a \equiv 0\ (m'); \quad x - a \equiv a_r - a\ (m_r)$$

zu vereinigen, was möglich ist, wenn $(m', m_r) \mid a_r - a$. Tatsächlich gehen wegen $a \equiv a_i \bmod m_i$ für $i = 1, \ldots r - 1$ alle (m_i, m_r) in $a_r - a$ auf, wenn (57) gilt, und damit auch ihr kl. gem. V. $m'' = \{(m_1, m_r), \ldots (m_{r-1}, m_r)\}$, das aber $= (m', m_r)$ ist: denn eine Primzahl p, die in m_r in der e-ten und in m_i in der e_i-ten Potenz aufgeht, geht sowohl in m'' als in (m', m_r) in der e-ten Potenz auf, wenn ein $e_i \geqq e$ ist, sonst aber, wenn alle $e_i < e$, in der höchsten der e_i-ten Potenzen.

Oft lautet die Aufgabe: alle Zahlen zu ermitteln, die je eine der Kongruenzen

$$x \equiv a_{11}, a_{12}, \ldots a_{1c_1} \bmod m_1, \ldots, x \equiv a_{r1}, \ldots a_{rc_r} \bmod m_r$$

erfüllen. Hierbei seien $a_{i1}, a_{i2}, \ldots$ untereinander inkongruente, zur Auswahl stehende Reste mod m_i, und die Verbindung je eines Restes mod m_1 bis mod m_r liefert eine simultane Kongruenz. Bei paarweis teilerfremden m_i hat man somit $c_1 c_2 \cdots c_r$ simultane Kongruenzen mit je einer Lösung mod $m = \Pi m_i$.

Beispiel: Es sollen alle „teilerfremden Reste" mod m ermittelt werden. (Der gr. gem. T. (a, m) hängt nur vom Rest a mod m ab!) Ist $m = p_1^{e_1} \cdots p_r^{e_r}$, so sind alle Werte

$$(58) \qquad x \not\equiv 0 \bmod p_1, \; x \not\equiv 0 \bmod p_2, \ldots, x \not\equiv 0 \bmod p_r$$

zu kombinieren. Es bleibt hier nur eine Aufgabe mod $p_1 p_2 \cdots p_r$ zu lösen. Nach diesem Modul gibt es $(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$ Werteverbindungen (58), also ebensoviel teilerfremde Reste mod Πp_i als Kongruenzlösungen von (58). Dies sind mod m

$$\varphi(m) = (p_1 - 1) \cdots (p_r - 1)\, \Pi p_i^{e_i - 1}$$

teilerfremde Reste, eine neue Ableitung für die Anzahl $\varphi(m)$. Die Bestimmungen der Lösungen vgl. § 34.

Ein Vertretersystem der teilerfremden Reste mod m heißt ein reduziertes Restsystem.

§ 16. Algebraische Kongruenzen. Lösungsanzahl.

Die Ergebnisse des vorigen Paragraphen werden wir nun verwenden, um Bedingungskongruenzen nach einem beliebigen Modul auf Kongruenzen nach Primzahlpotenzmoduln zurückzuführen, und für diese werden wir auch eine gewisse Zurückführung der Kongruenz mod p^e auf Kongruenzen mod p gewinnen und zwar folgender Art: Gilt $x \equiv a \bmod p^{e-1}$, so gilt eine der Kongruenzen

$$(59) \qquad x \equiv a + p^{e-1} y \bmod p^e, \quad y = 0, 1, \ldots p - 1.$$

Um also ein mod p^{e-1} bereits festliegendes x mod p^e festzulegen, ist noch eine zusätzliche Kongruenz für y mod p aufzustellen, und auf diese wird dann die ursprüngliche schrittweise zurückgeführt.

Besonders für algebraische Kongruenzen (solche zwischen Polynomen), die wir hier betrachten wollen, ist es wichtig, auf Kongruenzen nach einem Primzahlmodul p zu kommen; denn ist der Koeffizientenbereich der betrachteten Polynome ein Körper, hier Restklassenkörper mod p, so gelten die bekannten Sätze über die Lösungsschar eines linearen Gleichungssystems und die eindeutige Zerlegbarkeit der Polynome in unzerlegbare Faktoren. Wir werden diese nur für die Linearfaktoren mod p der Polynome einer Variabeln brauchen. Wir definieren

$$A(x_1, \ldots x_n) \equiv B(x_1, \ldots x_n) \bmod m, \tag{60}$$

wenn alle Koeffizienten von $A - B$ durch m teilbar sind. Also $\overline{A} = \overline{B}$ für die Polynome, deren Koeffizienten die zugehörigen Restklassen mod m sind; womit jede Kongruenz wieder eine Restklassengleichung darstellt.

Für ein Polynom in einer Variabeln x heißt f der *Grad* von $A(x) \bmod m$, wenn x^f die höchste in A vorkommende Potenz mit einem Koeffizienten $\not\equiv 0 \bmod m$ ist. Einem $A(x) \equiv 0 \bmod m$ sei kein Grad zugeordnet.

Beispiel: $12x^3 + 9x^2 + 4$ hat mod 5 den Grad 3, mod 4 den Grad 2, mod 3 den Grad 0 und ist z. B. $\equiv 2x^3 - x^2 - 1 \bmod 5$, $\equiv x^2 \bmod 4$, $\equiv 1 \bmod 3$. $x^3 - x$ hat mod 3 den Grad 3 und ist insbesondere $\not\equiv 0$, obwohl es für jedes $x \equiv 0, 1, 2$ den Rest 0 ergibt. Es können demnach verschiedene Restklassenpolynome an allen Stellen übereinstimmen. Vgl. hier § 18!

Wir behandeln jetzt die beiden Zurückführungsaufgaben und zwischen ihnen die Polynomkongruenz mod p.

Aufgabe A. Zurückführung der Lösung von Kongruenzen $A(x_1, \ldots x_n) \equiv 0 \bmod m$ auf Kongruenzen mod p^e.

Es sei $m = p_1^{e_1} \cdots p_r^{e_r}$; $p_i^{e_i} = m_i$, die Lösungen von $A(x_1, \ldots x_n) \equiv 0 \bmod m_i$ seien bekannt, und es sei

$x_1 \equiv x_1'$, $x_2 \equiv x_2'$, $\ldots$ $x_n \equiv x_n'$ irgendeine Lösung mod m_1;
$x_1 \equiv x_1''$, $x_2 \equiv x_2''$, $\ldots$ $x_n \equiv x_n''$ „ „ mod m_2;
. . . . . .
$x_1 \equiv x_1^{(r)}$, $x_2 \equiv x_2^{(r)}$, $\ldots$ $x_n \equiv x_n^{(r)}$ „ „ mod m_r.

Dann gibt es nach Satz 30 ein mod m eindeutig bestimmtes

x_k^0, das die Kongruenzen der k-ten Spalte dieses Schemas zugleich erfüllt. Dies für $k = 1, \ldots n$ durchgeführt ergibt die das Schema erfüllende Lösung $x_1 \equiv x_1^0, \ldots, x_n \equiv x_n^0 \bmod m$. Hat $A(x_k) \equiv 0 \bmod m_i$ genau c_i verschiedene Lösungen $(x_1, \ldots x_n)$, die also zu je zweien in irgendeiner Variabeln $x_k \bmod m_i$ abweichen, so lassen sich $c_1 \cdots c_r$ verschiedene Schemata aufstellen, deren Lösung x_k^0 jeweils $A(x_k) \equiv 0 \bmod m_i$ für alle i erfüllt und damit $A \equiv 0 \bmod m$. Es entstehen so $c_1 \cdots c_r$ verschiedene Lösungen $\bmod m$, die immer nach wenigstens einem m_i verschiedene Lösungen schon darstellen. Umgekehrt liefert jede Lösung $(x_1, \ldots x_n)$ von $A \equiv 0 \bmod m$, weil sie zugleich $A \equiv 0 \bmod m_i$ erfüllt, ein Lösungsschema obiger Art. Es gibt daher keine weiteren Lösungen, insbesondere überhaupt keine, sobald nur eine Kongruenz $A \equiv 0 (m_i)$ unlösbar ist. Wir haben:

Satz 32: Die Anzahl $a(m)$ der endlichvielen Lösungen einer Kongruenz $A(x_1, \ldots x_n) \equiv 0 \bmod m$ ist eine distributive Funktion von m. Man erhält alle Lösungen $\bmod m$ durch unabhängige Vereinigung der Lösungen nach den einzelnen Primpotenzteilern von m.

Auch für gemeinsame Lösungen mehrerer Kongruenzen $\bmod m$ ist die Anzahl distributiv. Und die Aufgabe wird einfacher, wenn man die Kongruenzen erst nach den $p_i^{e_i}$ löst, die gemeinsamen Lösungen aussiebt und dann zu Lösungen $\bmod m$ vereinigt. Eine Aussiebung ist bei Kongruenzen, wo es sich um endlich viele, oft nur sehr wenige Lösungen handelt, meist einem algebraischen Verfahren vorzuziehen.

Beispiel: $x^2 + y^2 \equiv 7 \bmod 15$.

Zerlegung: $x^2 + y^2 \equiv 1 \bmod 3$; $\equiv 2 \bmod 5$.

Lösungen mod 3: $x \equiv 0, y \equiv \pm 1$ oder umgekehrt. $a = 4$.

„ mod 5: $x \equiv \pm 1, y \equiv \pm 1$, unabh. kombin. $a = 4$.

„ mod 15: $x \equiv \pm 6, y \equiv \pm 1, \pm 4$ $a = 16$.
oder umgekehrt, bei unabh. Kombination.

Weiterhin nur Polynome einer Variabeln betrachtend bestimmen wir, als allgemeines Beispiel, die

Anzahl der Lösungen der Kongruenz $x^2 \equiv 1 \bmod m$.

Für eine Lösung x mod p^e muß gelten

(61) $$p^e \mid x^2 - 1 = (x-1)(x+1).$$

Ist $p > 2$, so geht p nicht zugleich in $x-1$ und $x+1$ auf; also gilt entweder $p^e \mid x-1$ oder $p^e \mid x+1$. Man hat die zwei Lösungen $x \equiv \pm 1 (p^e)$.

Für $p = 2$ und $e = 1$ ist $x \equiv +1 \equiv -1 \bmod 2$ die einzige Lösung; bei $e = 2$, also mod 4, sind das wieder zwei Lösungen; für $e \geqq 3$ kommen nun noch neue Lösungen hinzu; es sind $x-1$ und $x+1$ zugleich gerade, jedoch nur eine der beiden Zahlen durch 4 teilbar. Diese muß daher durch 2^{e-1} teilbar sein, und das genügt, damit $x^2 - 1$ durch 2^e teilbar. Man hat

$$x \equiv \pm 1 \bmod 2^{e-1}, \quad \equiv \pm 1, \quad \pm 1 + 2^{e-1} \bmod 2^e$$

als die Lösungen von $x^2 \equiv 1 \bmod 2^e$, und dies sind mod 2^e vier inkongruente Lösungen, sobald $e > 2$. Für $e = 3$, $m = 8$, sind noch alle primen Reste 1, 3, 5, 7 Lösungen. Für $m = 16$ nur noch die Reste 1, 7, 9, 15.

Für beliebiges m ist nun Satz 32 anzuwenden; man erhält, wenn $m = 2^s p_1^{e_1} \cdots p_1^{e_r}$, p_i die ungeraden Primteiler von m, $e_i > 0$ und $s \geqq 0$, 2^r Lösungen für $s < 2$, 2^{r+1} Lösungen für $s = 2$ und 2^{r+2} für $s > 2$. Durch Vereinigung der Primpotenzmodullösungen erhält man z. B. für $x^2 \equiv 1$

mod 45: vier Lösungen $x \equiv \pm 1, \pm 19 (45)$;

mod 120: 16 „ , zusammenfaßbar in $x \equiv \pm 1, \pm 19 (30)$.

Aufgabe B. Behandlung der Kongruenz $A(x) \equiv 0 \bmod p$.

$$A(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

Für die Lösungen (Wurzeln) der Kongruenz, die sich durch Einsetzen eines vollständigen Restsystems mod p für x feststellen lassen, bestehen folgende Zusammenhänge:

Satz 33: Es ist r genau dann Wurzel einer Kongruenz $A(x) \equiv 0$ nach irgendeinem Modul m, wenn $A(x) \equiv (x-r) Q(x) \bmod m$ zerlegbar ist.

Beweis: Für jedes r gilt, sogar als Gleichung,

$$A(x) - A(r) = (x^n - r^n) + a_1 (x^{n-1} - r^{n-1}) + \cdots + a^{n-1}(x-r)$$
$$= (x-r) Q_r(x) \text{ wegen } x - r \mid x^i - r^i.$$

Für $A(r) \equiv 0 \bmod m$ ist daher $A(x) \equiv (x - r)\, Q_r(x)$; die Umkehrung ist klar.

Satz 34: Sind $r_1, r_2, \ldots r_k$ einander inkongruente Lösungen von $A(x) \equiv 0 \bmod p$ und p eine Primzahl, so gilt eine Kongruenz

$$(62) \qquad A(x) \equiv (x - r_1)\,(x - r_2) \cdots (x - r_k)\, A_k(x).$$

Ist nämlich $A(x) \equiv (x - r_1) \cdots (x - r_i)\, A_i(x)$ und r eine zu r_1 bis r_i inkongruente Lösung von $A(x) \equiv 0 \bmod p$, so folgt aus $A(r) \equiv (r - r_1) \cdots (r - r_i)\, A_i(r) \equiv 0$, aber $r - r_1, \ldots, r - r_i \not\equiv 0$, daß $A_i(r) \equiv 0$, weil p Primzahl. Also gilt für die zu r_1 bis r_i hinzukommende Kongruenzwurzel r nicht nur $x - r \mid A(x)$, sondern auch $x - r \mid A_i(x)$. Induktionsschluß liefert jetzt (62).

Folgerung: Eine Kongruenz n-ten Grades hat höchstens n Wurzeln mod p und zerfällt in diesem Falle

$$(63) \qquad A(x) \equiv (x - r_1)\,(x - r_2) \cdots (x - r_n).$$

Anwendung: Für jeden teilerfremden Rest r gilt eine Kongruenz $r^h \equiv 1\,(p)$, da $r, r^2, \ldots r^m, \ldots$ nicht alle einander inkongruent sein können und mit $r^m \equiv r^n$ bei $m > n$ zugleich $r^{m-n} \equiv 1\,(p)$. Das kleinste h dieser Eigenschaft heißt der *Exponent* oder die *Ordnung* von r mod p. Es gilt dann

$$(64) \qquad r^h \equiv r^{2h} \equiv r^{3h} \equiv \cdots \equiv 1.$$

Während $1, r, r^2, \ldots r^{h-1}$ untereinander inkongruent sind, weil sonst unter ihnen ein Quotient $r^{m-n} \equiv 1$ mit $m - n < h$ vorkäme. Alle Potenzen von r genügen nach (64) der Kongruenz $x^h - 1 \equiv 0\,(p)$, und h ist zugleich die Anzahl der inkongruenten; daher gilt mit (63)

$$(65) \qquad x^h - 1 \equiv (x - 1)\,(x - r)\,(x - r^2) \cdots (x - r^{h-1}),$$

wenn r mod p zum Exponenten h gehört. — Ferner

Satz 35: Zerfällt $A \equiv BC \bmod p$, so ist nicht nur jede Wurzel von $B(x) \equiv 0$ oder $C(x) \equiv 0$ eine der Wurzeln r_i von $A(x) \equiv 0$, sondern es kommt auch jedes r_i bei B oder C als Wurzel vor. Gilt insbesondere (63), so sind B und C mod p je ein Produkt dieser Linearfaktoren.

Ist nämlich $B(r_i) \not\equiv 0$, so ist mit $A(r_i)$ auch $C(r_i)$ durch p teilbar, also der erste Teil von Satz 35 richtig. Für (63) seien r_1 bis r_m die Wurzeln von $B \equiv 0$. Dann müssen die übrigen r_i Wurzeln von $C \equiv 0$ sein und, weil BC nur den Grad n hat,

$$B \equiv \prod_{i \leq m} (x - r_i) \cdot 1, \quad C \equiv \prod_{i > m} (x - r_i) \cdot 1.$$

Aufgabe C. Zurückführung der Lösung von Kongruenzen mod p^e auf Kongruenzen mod p^{e-1}. $(e > 1.)$

Es seien $r_1, r_2, \ldots r_k$ mod p^{e-1} ein vollständiges System inkongruenter Lösungen der Kongruenz $A(x) \equiv 0 \ (p^{e-1})$:

$$(66) \qquad A(x) = (x - r_i) Q_i(x) + A(r_i) \quad \text{mit } p^{e-1} \mid A(r_i).$$

Nun kommt es darauf an, ob $Q_i(r_i) \not\equiv 0$ oder $\equiv 0 \bmod p$ (in algebraischer Sprechweise: ob r_i „einfache" oder „mehrfache" Wurzel von $A(x) \equiv 0 \bmod p$ ist).

Im ersten Fall entspricht der Lösung r_i mod p^{e-1} genau eine Lösung $r_i' \equiv r_i + p^{e-1} y \bmod p^e$ (y irgend ein Rest mod p).

Setzt man nämlich r_i' mit beliebigem y an, so wird nach (66), wenn $Q_i(r_i) \equiv c \bmod p$,

$$(67) \qquad \begin{aligned} A(r_i') &= (r_i' - r_i) Q_i(r_i') + A(r_i) \\ &\equiv p^{e-1} y \cdot c + p^{e-1} a \mod p^e. \end{aligned}$$

(Es gilt auch $Q(r_i') \equiv c \bmod p$ wegen $r_i' \equiv r_i (p)$.) Nach Voraussetzung ist $c \not\equiv 0 (p)$ und daher $y \cdot c \equiv -a$ für genau ein $y \bmod p$ erfüllt, und dies liefert $A(r_i') \equiv 0 \ (p^e)$.

Zweiter Fall: $Q_i(r_i) \equiv 0 \bmod p$. Nach (67) wird:

$$A(r_i') \equiv p^{e-1} a \ (p^e) \quad \text{für jedes } r_i' \equiv r_i \ (p^{e-1}).$$

Also ist jedes r_i' Lösung, wenn $a \equiv 0 (p)$, sonst keins.

Von den einzelnen Kongruenzwurzeln mod p zu denen mod p^e in $e - 1$ Schritten aufsteigend, erhält man bei festbleibendem $Q_i \equiv c \bmod p$ insgesamt:

Satz 36: Seien $r_1, \ldots r_k$ sämtliche Kongruenzwurzeln von $A(x) \equiv 0 \bmod p$, und alle Wurzeln „einfach", d. h.

$$A(x) \equiv (x - r_1)(x - r_2) \cdots (x - r_k) Q(x) \bmod p$$

mit $Q(r) \not\equiv 0 (p)$ für alle Reste r, so gibt es auch genau k Lösungen mod p^e, die aus den Lösungen

nach den niederen Potenzen von p schrittweise hervorgehen: die zu r_i gehörige Lösung mod p^e unterscheidet sich von der mod p^{e-1} höchstens um ein Vielfaches von p^{e-1}.

Ist allgemein r_i einfache, r_j mehrfache Wurzel mod p, also $Q(r_i) \not\equiv 0$, $Q(r_j) \equiv 0 \bmod p$, so hat $A \equiv 0 \bmod p^e$ genau eine Wurzel, die $\equiv r_i \bmod p$, dagegen Wurzeln $\equiv r_j \bmod p$ entweder keine oder Scharen von je p Wurzeln desselben Restes mod p^{e-1}.

Von zwei Lösungen mod p^{e-1}, die aus einer mehrfachen Wurzel mod p hervorgehn, kann sehr wohl die eine ohne die andere Lösung mod p^e sein (Beispiel 3, 4), da $A(r_i)$ in (66) nicht nur von $r_i \bmod p$ abhängt.

Beispiele (wir wählen $p = 3$):

1. $x^2 + 11 \equiv 0 \bmod 3^e$. Zwei einfache Wurzeln $x \equiv \pm 1, 4, 4, 31, 31, 274 \ldots \bmod 3, 9, 27, 81, 243, 729, \ldots$

2. $A(x) \equiv x^2 + x + 1 \equiv 0$. $A(x) = (x-1)(x+2) + 3$. Eine mehrfache Wurzel $+1 \bmod 3$, schon keine Wurzel mod 9.

3. $x^3 - 19 \equiv 0\ (3^e)$. Mehrfache Wurzel:

$$x \equiv \underline{1} \bmod 3;\ 1, 4, \underline{7}, \bmod 9;\ 7, 16, 25 \bmod 27; \ldots.$$

(Die Lösungen, aus denen die der höheren Potenz hervorgehn, sind unterstrichen. Diese Werte sind dann auch jeweils in (66) für r_i einzusetzen.)

4. $A(x) \equiv x(x-1)(x-4) \equiv 0 \bmod 3^e$. Eine einfache Wurzel $0 \bmod 3^e$; eine mehrfache Wurzel $x \equiv \underline{1} \bmod 3$; $\underline{1}, 4, 7 \bmod 9$; $\underline{1}, \underline{4}, 10, 13, 19, 22 \bmod 27$; $\underline{1}, \underline{4}, 28, 31, 55, 58 \bmod 81; \ldots$.

§ 17. Der Fermatsche Satz.

Wir kommen nun zu dem Satz der Kongruenzlehre, der für fast alle weiteren Ergebnisse grundlegend ist, dem Fermatschen Satz. Er lautet:

Satz 37: Für jede Primzahl p und jeden Rest x mod p gilt die Kongruenz

$$x^p \equiv x \bmod p. \tag{68}$$

Oder für jeden zu p teilerfremden Rest r

$$r^{p-1} \equiv 1 \bmod p. \tag{69}$$

Dieser von Fermat (1601—65) aufgestellte und bewiesene Satz wird oft der „kleine Fermat“ genannt; dagegen wird als „großer Fermat“ eine von Fermat aufgestellte, immer noch unbewiesene Behauptung bezeichnet, daß $x^n + y^n = z^n$ für $n > 2$ in ganzen Zahlen x, y, z unlösbar sei. Für einzelne n ist der Beweis gelungen, oft mit großen Schwierigkeiten; $n = 4$ vgl. § 20. An Wichtigkeit ist der große Fermat dem kleinen Fermat weit unterlegen.

Um den Fermatsatz in der Form (68) zu beweisen, beachte man, daß allgemein

$$(70) \qquad (x + y)^p \equiv x^p + y^p \bmod p$$

für Zahlen, Variable, Polynome x, y gilt. Nämlich $x^{p-i} y^i$ hat für $i = 1, 2, \ldots$ einen Koeffizienten

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i} \equiv 0 \bmod p \quad \text{für} \quad i < p.$$

Für $y = 1$ gilt also $(x+1)^p \equiv x^p + 1^p \equiv x + 1 \bmod p$ mit $x^p \equiv x$. Dies liefert einen Induktionsbeweis für (68); die Anwendung der Induktion darf sich dabei auf ein vollständiges Restsystem mod p beschränken.

Ein andrer Beweis, der auf (69) ausgeht, liefert zugleich den allgemeineren Eulerschen Satz:

Satz 38: Ist $\varphi(m)$ die Anzahl der teilerfremden Reste mod m und r einer von diesen, so gilt

$$(72) \qquad r^{\varphi(m)} \equiv 1 \bmod m.$$

Beweis: Sei $r_1, r_2, \ldots r_\varphi$ ein reduziertes Restsystem mod m und r einer dieser Reste, so gilt

$$(73) \qquad r r_1 \cdot r r_2 \cdots r r_\varphi \equiv r_1 \cdot r_2 \cdots r_\varphi;$$

denn links steht in (73) gerade jeder zu m fremde Rest in der Form $r r_i$ einmal da, weil die Kongruenz $rx \equiv r_k \bmod m$ genau eine Lösung $x \equiv r_i \smile m$ hat. Also ist nach (73)

$$r^\varphi \cdot r_1 \cdots r_\varphi \equiv r_1 \cdots r_\varphi,$$

und das liefert (72).

Eine unmittelbare Folge von Satz 37 ist, daß der Exponent h eines teilerfremden Restes r ein Teiler von $\varphi(m)$ ist, da $\varphi(m)$ unter der Exponentenreihe (64) vorkommen muß.

Ebenfalls ist der „gemeinsame Exponent" aller teilerfremden Reste, die kleinste Zahl $\psi(m)$, für die alle $r \smile m$ die Kongruenz $r^{\psi(m)} \equiv 1 \bmod m$ erfüllen, als kl. gem. V. der Exponenten von r_1 bis r_φ ein Teiler von $\varphi(m)$. Es fragt sich: für welche m ist $\psi(m)$ ein echter Teiler von $\varphi(m)$, läßt sich mithin das Ergebnis (72) verschärfen, und wann ist $\psi(m) = \varphi(m)$? Vor allem gilt da

Satz 39: Ist $\psi(m)$ der kleinste Exponent, der (72) an Stelle von $\varphi(m)$ erfüllt, und ist $m = q_1 \cdots q_s$ die Primpotenzzerlegung von m, so gilt

$$\psi(m) = \{\psi(q_1), \ldots, \psi(q_s)\}. \tag{74}$$

Ist nämlich v durch alle $\psi(q_i)$ teilbar, so gilt $x^v \equiv 1 \bmod q_i$ $(i = 1, \ldots s)$, also mod m, für jedes $x \smile m$. Und umgekehrt.

Aus (74) schließt man sofort, daß $\psi(m)$ echter Teiler von $\varphi(m)$, sobald mehrere $q_i > 2$; denn $\psi(m)$ ist nach (74) wegen $\psi(q) \mid \varphi(q)$ ein Teiler von $\{\varphi(q_1), \ldots \varphi(q_s)\}$ und dies ein Teiler des halben Produktes $\prod \varphi(q_i) = \varphi(m)$, weil $\varphi(q_1)$ und $\varphi(q_2)$ gerade sind, wenn $q_1, q_2 > 2$.

Auch für $m = 2^e$ und $e \geqq 3$ ist $\psi(m) \mid \frac{1}{2}\varphi(m)$. Denn nach § 16 ist $x^2 \equiv 1 \bmod 8$ und dann $x^4 \equiv 1 \bmod 16$, $x^8 \equiv 1 \bmod 32, \ldots$ $x^{2^{e-2}} \equiv 1\,(2^e)$, weil nach (61) allgemein $z^2 \equiv 1 \bmod 2^s$, wenn $z \equiv 1 \bmod 2^{s-1}$. Umgekehrt galt $z^2 \equiv 1 \bmod 2^s$ nur für $z \equiv \pm 1 \bmod 2^{s-1}$. Daher gehört 9 mod 2^e zum Exponenten 2^{e-3} und 3 zu 2^{e-2}. Es ist also $\psi(2^e) = 2^{e-2} = \frac{1}{2}\varphi(2^e)$ für $e \geqq 3$.

Hingegen werden wir $\psi(q) = \varphi(q) = \psi(2q) = \varphi(2q)$ in § 18 für ungerade Primpotenzen q zeigen. Daher

$$\psi(m) = \{\psi(2^e), \varphi(q'), \varphi(q''), \ldots\} \tag{75}$$

bei $m = 2^e q' q'' \cdots$, $e \geqq 0$; $\psi(2^e) = \frac{1}{2}\varphi$ für $e \geqq 3$, sonst $= \varphi$.

Es ist $\psi = 1,\ 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 16$
noch für $m = 2, 24, 240, 504, 480, 264, 65520, 16320$.

Wir werden bald zeigen, daß es immer einen Rest der Ordnung $\psi(m)$ gibt, der dann für $\psi = \varphi$ alle teilerfremden Reste durch seine Potenzen darstellt.

Anwendung des Fermatsatzes auf periodische Dezimalbrüche:

Ohne auf die Entstehung der unendlichen Dezimalbrüche näher einzugehen, stellen wir fest: Der periodische Dezimalbruch

$$w = 0, c_1 c_2 \cdots c_k \overline{a_1 a_2 \cdots a_n}$$

mit Ziffern c und a von 0 bis 9 und der immer wiederkehrenden Folge $a_1, \ldots a_n$ stellt den echten Bruch

$$\frac{c_1 c_2 \cdots c_k}{10^k} + \frac{a_1 a_2 \cdots a_n}{10^k (10^n - 1)}$$

mit im Dezimalsystem geschriebenen Zähler dar, und es wird $10^k (10^n - 1)\, w$ eine ganze Zahl. — Umgekehrt ist jede Rationalzahl $r = g + w$ darstellbar, wo g ganz und w ein periodischer Dezimalbruch wie oben: Jedenfalls ist $r = g + l : 10^k m$ darstellbar mit eindeutigem g, k, l, m bei $(m, l) = (m, 10) = 1$, $l \not\equiv 0\ (10)$ und $< 10^k m$. Ist dann n der Exponent von $10 \bmod m$, so ist sicher $m \mid 10^n - 1$ und

$$\frac{l}{m} = c_1 \cdots c_k + \frac{a_1 \cdots a_n}{10^n - 1}$$

darstellbar, somit $r = g + w$ mit obigem w. Die Periode fängt noch nicht früher an, d. h. es ist $c_k \neq a_n$; denn sonst reichte 10^{k-1} im r-Nenner, entgegen $l \not\equiv 0\ (10)$. Und Periodenlänge ist wirklich m, es liegt also keine mehrfache Wiederholung einer kürzeren Periode etwa der Länge h vor; denn dann wäre bereits $10^k (10^h - 1)\, w$ ganz und $m \mid 10^h - 1$ wegen $(m, 10\, l) = 1$, während doch n die kleinste Zahl mit $m \mid 10^n - 1$ ist.

Nach dem Fermatsatz ist n ein Teiler von $\varphi(m)$. Es ist $n = \varphi(m)$ z. B. für die Potenzen von 7, 17, 19. Es wird

$n = 1$ für $m = 3, 9$; $n = 2$ für $m = 11$; 3 für 27, 37;
4 für 101; 5 für 41, 271; 6 für 7, 13.

Daraus nach (75) z. B. $n = 12$ für $1 : 2727$, $n = 6$ für $1 : 481$.

§ 18. Primitivwurzeln. Restklassengruppe.

Primitivrest oder Primitivwurzel mod m heißt ein Rest v, dessen Potenzen alle teilerfremden Reste mod m darstellen. Kennzeichen dafür ist, daß er zum Exponenten $\varphi(m)$ gehört.

Satz 40: Das Polynom $x^{p-1} - 1$ zerfällt mod p linear:

$$(76)\quad x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \bmod p.$$

($x^p - x$ ist also das Produkt aller inkongruenten Linearfaktoren mod p.) Genau $\varphi(p-1)$ Reste sind Primitivwurzeln.

Ebenso besitzt ein ungerader Primpotenzmodul $q = p^e$ Primitivwurzeln und zwar

$$\varphi(\varphi(p^e)) = \varphi(p-1) \cdot (p-1)\, p^{e-2}.$$

Für $e \geqq 2$ sind es die Reste, die mod p Primitivwurzeln sind, aber nicht der Kongruenz $x^{p-1} \equiv 1 \bmod p^2$ genügen.

Beweis für p: Die Kongruenz (76) folgt aus dem Fermatsatz in Verbindung mit Satz 34; es tritt Fall (63) ein.

Ist $f(t)$ die Anzahl der Reste mod p, die zum Exponenten t gehören, so ist $F(d) = \Sigma f(t)$, $t \mid d$, die Anzahl der Wurzeln der Kongruenz $x^d - 1 \equiv 0$. Ist nun $d \mid p-1$, so wird $F(d) = d$; denn dann ist $x^d - 1$ als Teiler von $x^{p-1} - 1$ nach Satz 35 ebenfalls ein Produkt von Linearfaktoren mod p. Nach Satz 25/23 ist dann $f(t) = \varphi(t)$ für die Teiler t von $p-1$, insbesondere $f(p-1) = \varphi(p-1)$ die Anzahl der Primitivwurzeln für p.

Man beachte: es ist $f(t) = \varphi(t)$ nur für $t \mid p-1$, sonst $= 0$; daher allgemein $F(n) = (n, p-1)!$ — Setzt man $x = 0$ in (76), so erscheint von neuem der Wilsonsche Satz.

Mod p^2: Damit alle teilerfremden Reste als Potenzen eines Restes v darstellbar seien, muß dieser sicher Primitivrest mod p sein. Ist nun die Zahl w ein Primitivrest mod p, so erfüllt genau eines der $w(1 + yp)$, $y = 0, 1, \ldots p-1$, die Kongruenz $x^{p-1} - 1 \equiv 0 \bmod p^2$, wie auch Satz 36 liefert, doch unmittelbar so folgt: Für $w^{p-1} = 1 + ap$ ist

$$(77) \quad w^{p-1}(1+yp)^{p-1} = (1+ap)(1+(p-1)yp + zp^2) \equiv 1 + (a-y)p \bmod p^2,$$

w also vom Exponenten $p-1$ mod p^2 für $y \equiv a$. Die übrigen $v = w(1+yp)$ sind wirklich Primitivwurzeln mod p^2: es ist $v^h \equiv 1 \bmod p$ schon nur für $p-1 \mid h$, mit (77) aber

$$(78) \quad v^{(p-1)l} \equiv 1 + l(a-y)p \bmod p^2,$$

also erst $v^{(p-1)p} \equiv 1 \bmod p^2$.

Über die Kongruenz $r^{p-1} \equiv 1\,(p^2)$ vgl. Kap. VI.

Mod p^e bleibt bei $e, p > 2$ jede Zahl v Primitivrest, die es mod p^2 ist: Allgemein ist bei $p = 2k+1$

$$(79)\qquad \begin{aligned}(1+zp^s)^p &= 1 + zp^{s+1} + z^2 kp^{2s+1} + yp^{3s}\\ &\equiv 1 + zp^{s+1} \mod p^{s+2}.\end{aligned}$$

Ist nun $v^{p-1} = 1 + zp$, so also $v^{(p-1)p} \equiv 1 + zp^2\,(p^3)$ und allgemein $v^{(p-1)p^{e-2}} \equiv 1 + zp^{e-1} \mod p^e$; dabei $z \not\equiv 0\,(p)$, wenn v Primitivrest mod p^2. Daraus folgt aber, daß v mod p^e wirklich zum Exponenten $(p-1)\,p^{e-1}$ gehört; denn für $v^h \equiv 1\,(p^e)$ muß wieder $p-1 \mid h$ gelten, und $h = (p-1)\,p^{e-2}$ reicht nicht aus.

Hiermit ist Satz 40 bewiesen. Man folgert aus ihm: Die Wurzeln der Kongruenz $x^{p-1} - 1 \equiv 0\,(p^e)$ gehen aus denen mod p (die ein reduziertes Restsystem durchlaufen) durch Erhebung in die p^{e-1}-te Potenz hervor. Jedoch findet für $q = p^e > p$ keine Übereinstimmung zwischen $x^{\varphi(q)} - 1$ und dem Produkt seiner Linearfaktoren $x - v^i$ mehr statt.

Ferner läßt sich jetzt leicht mod m ein Rest mit der in (75) angegebenen Ordnung $\psi(m)$ bestätigen: mod 2^e hatte 3 (auch 5) diese Eigenschaft und mod q jeder Primitivrest. Ist $m = 2^e q_1 \ldots q_s$ und v_i Primitivrest mod q_i, so hat

$$v \equiv 3\ (8),\quad v \equiv v_1(q_1), \ldots \quad v \equiv v_s(q_s)$$

eine Simultanlösung der Ordnung $\psi(m)$ mod m; denn $v^h \equiv 1 \mod 2^e \Pi q_i$ erfordert $\psi(2^e), \varphi(q_i) \mid h$. Wichtiger ist folgende Anwendung simultaner Kongruenzen auf Primitivwurzeln: Ein Rest $r \smile m = 2^e q_1 \cdots q_s$ ist darstellbar

$$(80)\qquad r \equiv r_0 r_1 \cdots r_s\,(m) \quad \begin{matrix}\text{mit } r_0 \equiv r\,(2^e),\ \equiv 1\,(q_1 \cdots q_s);\\ \text{und } r_i \equiv r\,(q_i),\ \equiv 1\,(m : q_i).\end{matrix}$$

Dabei
$$r_i = v_i^{e_i} \text{ mit } v_i \equiv v\,(q_i),\ \equiv 1\,(m : q_i);$$
$$r_0 = v_0^{e_0} \text{ mit } v_0 = 4q_1 \cdots q_s + 1,$$

für $4 \mid m$ nur r oder $-r$. D. h. löst man die simultanen Kongruenzen rechts in (80), so erhält man die Darstellungen links, als multiplikatives Gegenstück zu (53), (54); es gilt

Satz 41: Jeder zu m teilerfremde Rest ist darstellbar

$$(81) \qquad r \equiv (-1)^c v_0^{c_0} v_1^{c_1} \cdots v_s^{c_s} \mod m = 2^e q_1 \cdots q_s$$

mit Hilfe der „Basis" $-1, v_0, v_1, \ldots v_s$, wie unter (80) definiert. Dabei ist die volle Basis nur für $8 \mid m$ zur Darstellung der gesamten reduzierten Restklassengruppe mod m („Gruppe" wegen umkehrbar ausführbarer Multiplikation) nötig. Für $e = 2$ fällt v_0 und für $e < 2$ außerdem -1 aus der Basis heraus. Sodann sind die in (81) zur Darstellung verwandten Exponenten nach ihren Ordnungen eindeutig: $c \bmod 2$, $c_0 \bmod 2^{e-2}$, $c_i \bmod \varphi(q_i)$ eindeutig.

(Um also eine eindeutige Darstellung (81) zu erhalten, darf man für den Exponenten c_i ein vollständiges Restsystem nach der Ordnung von v zulassen und für c bei $4 \mid m$ die Werte 0 und 1; sonst aber nur $c = 0$, weil dann $-1 = v_1^{t_1} \cdots v_s^{t_s} \bmod m$ mit $t_i = \frac{1}{2}\varphi(q_i)$.)

Der Fall der eingliedrigen Basis ist durch die Existenz einer Primitivwurzel v ausgezeichnet; (81) geht über in

$$(82) \qquad r \equiv v^c, \quad 0 \leqq c < \varphi(m).$$

Hier nennt man c bei fester Basis v den *Index* von $r \bmod m$ und schreibt $c = \operatorname{ind} r$. Indextafeln sind für Kongruenzrechnungen oft wertvoll; ihre Berechnung vgl. § 37. Wir stellen hier je eine mod 7, 9, 13 auf:

$m = 7;\ v = 3$						
r	1	2	3	4	5	6
c	0	2	1	4	5	3

$m = 9;\ v = 2$						
r	1	2	4	5	7	8
c	0	1	2	5	4	3

r	1	2	3	4	5	6	7	8	9	10	11	12	$m = 13$
c	0	1	4	2	9	5	11	3	8	10	7	6	$v = 2$

§ 19. Potenzreste.

Ein teilerfremder Rest $a \bmod m$ heißt *n-ter Potenzrest* $\bmod m$, wenn die Kongruenz

$$(83) \qquad x^n \equiv a \mod m$$

lösbar ist, also mit einem zu m fremden x. Die teilerfremden Reste stehen gerade bei dieser Frage so im Vordergrund —

und man wird die Lösung von (83) für anderes a wie in § 21 immer auf den Fall $a \smile m$ zurückführen — daß nur auf diese die Bezeichnung „n-ter Potenzrest" angewandt wird. In der Theorie der Potenzreste sind die Hauptfragen:

A. Welches sind die n-ten Potenzreste mod m?

B. Für welche Moduln m ist a ein n-ter Potenzrest?

(C. Ein wie hoher Potenzrest ist $a \bmod m$?)

Während A. und C. durch Ausrechnung zu beantworten sind, ist B. für $n > 2$ eine Frage, die höhere zahlentheoretische Hilfsmittel zur Beantwortung erfordert. Man wird die Fragen aber sofort auf den Fall des Primpotenzmoduls zurückführen, da (83) für $m = q_1 \cdots q_s$ gleichwertig mit

$$x^n \equiv a \bmod q_1, \ldots \; x^n \equiv a \bmod q_s.$$

Für einen ungeraden Primzahlpotenzmodul q gilt nun das allgemeine *Eulersche Kriterium*:

Satz 42: Die Zahl a ist genau dann n-ter Potenzrest mod $q = p^e$, $p > 2$, wenn

$$(84) \qquad a^{\varphi_n(q)} \equiv 1 \bmod q \quad \text{bei} \quad \varphi_n(q) = \varphi(q) : (n, \varphi).$$

$\varphi_n(q) = (n, \varphi(q))$ ist dabei zugleich die Anzahl der Lösungen der Kongruenz $x^n \equiv 1\,(q)$.

Für $q = 2^e$ ($e \geqq 2$, n gerade) muß außerdem $a \equiv 1\,(4)$ sein, und dann gilt für a das Kriterium (84) mit 2^{e-2} statt φ. (Beide Fälle zusammengefaßt: (84) mit $\psi(q)$ statt $\varphi(q)$ und $a \equiv 1\,(4, 2n, q)$ für n-ten Potenzrest a.)

Beweis: Tatsächlich ist für $(n, \psi(q)) = n'$ bereits jeder n'-te Potenzrest ein n-ter Potenzrest; denn aus $a \equiv z^{n'}$ folgt bei $n' = cn + k\psi$ zugleich $a \equiv z^{cn}$. *Eigentlich sinnvoll* ist daher die *Potenzrestfrage nur für* $n \mid \psi(q)$, insbesondere $n \mid 2^{e-2}$ für $q = 2^e$. Während jede Zahl n-ter Rest ist, wenn $(n, \varphi) = 1$. Für $4 \mid q$ ist daher, wie oben durch $a \equiv 1\,(4, 2n, q)$ vermerkt, $a \equiv 1\,(4)$ nur für gerades n zu fordern und nur da (84) zu untersuchen.

Mit Hilfe der Indexrechnung (für $q = 2^e$ mit der Basis 5) schließen wir nun: (84) ist gleichbedeutend mit

$$\psi_n \operatorname{ind} a \equiv 0 \mod \psi;$$

und dies mit $\operatorname{ind} a \equiv 0 \bmod \psi : \psi_n = n'$, und das heißt, daß a ein n'-ter Potenzrest ist, was von (84) noch zu beweisen blieb.

Daß n' für ungerades q zugleich die Anzahl der Lösungen der Kongruenz $x^n \equiv 1\,(q)$ ist, folgt ebenso: es ist

$$n \operatorname{ind} x \equiv 0 \bmod \psi(q)$$

zu erfüllen oder $\operatorname{ind} x \equiv 0\,(\psi : n')$. Dies ergibt n' Lösungen $\operatorname{ind} x = z\psi_n$ mit $0 \leqq z < n'$.

Für $q = 2^e$ ist entsprechend $n' = (n, \psi(q))$ die Anzahl der Lösungen von $x^n \equiv 1\,(q)$; $x \equiv 1\,(4, q)$, für $4 \mid q$ und gerades n also $2n'$ die Lösungszahl von $x^n \equiv 1\,(q)$, weil dann $(-x)^n = x^n$, somit zu jeder Lösung x, die außerdem $\equiv +1 \bmod 4$, eine Lösung $-x \equiv -1\,(4)$ hinzutritt.

Für einen beliebigen Modul m gilt nur:

Satz 43: Ein n-ter Potenzrest $a \bmod m$ muß die Kongruenz $x^N \equiv 1 \bmod m$ erfüllen; N Anzahl der n-ten Potenzreste. Zugleich gilt $N \cdot \chi_n(m) = \varphi(m)$, wo $\chi_n(m)$ die Lösungsanzahl der Kongruenz $x^n \equiv 1 \bmod m$.

Beweis: Sind $a_1, a_2, \ldots, a_N$ alle n-ten Potenzreste und a einer von ihnen, so stellen $aa_1, \ldots, aa_N$ wieder alle n-ten Reste dar, weil $aa_i \equiv (xy)^n$ mit $a \equiv x^n$ und $a_i \equiv y^n$. Also $\Pi a_i \equiv a^N \Pi a_i$; $a^N \equiv 1$.

Ferner folgt $N \cdot \chi_n = \varphi$ daraus, daß χ_n für jeden n-ten Rest a die Anzahl der Lösungen von $x^n \equiv a\,(m)$ ist, und das folgt so: durchläuft z_i alle Lösungen der Kongruenz $x^n \equiv 1\,(m)$, und ist y eine Lösung von $x^n \equiv a\,(m)$, so auch jedes yz_i, und das sind alle Lösungen, da umgekehrt der Quotient zweier Lösungen dieser Kongruenz eine Lösung von $x^n \equiv 1$ ist.

Für Primzahlmoduln m gewinnt man so einen neuen, die Existenz einer Primitivwurzel nicht verwendenden Beweis von Satz 42: wenn man hinzufügt, daß die Kongruenz $x^N \equiv 1 \bmod p$ nur N Wurzeln haben kann und daher auch jede dieser Wurzeln einer der N n-ten Potenzreste sein muß.

Schließlich liefert die Distributivität der Lösungsanzahl (Satz 32), weil $\chi_n(q) = (n, \varphi(q))$ für $q = p^e$, jedoch $= 2(n, \psi(q)) = (2n, \varphi(q))$ für $4 \mid q$ und gerades n:

Satz 44: Für jeden n-ten Potenzrest $a \bmod m$ ist die Anzahl der Lösungen der Kongruenz $x^n \equiv a \bmod m$,

wenn $m = q_1 \dots q_s$ in Primpotenzen einschließlich Zweierpotenzen zerfällt:

$$\chi_n(m) = \prod_{i=1}^{s} (n(2, n, q_i), \varphi(q_i)). \tag{85}$$

§ 20. Quadratsummendarstellung.

Wir bringen jetzt noch Anwendungen des abzählenden Schubfächerprinzips in Kongruenzen, die vom multiplikativen Fermatsatz unabhängig sind. Wir werden beweisen:

Satz 45: Jede Primzahl p der Form $4n+1$ ist die Summe zweier Quadrate: $p = x^2 + y^2$.

Satz 46: Die Primzahlen p der Form $4n+1$ und ihre Doppelten sind dadurch gekennzeichnet, daß sie genau eine Darstellung der Form $x^2 + y^2$ mit $(x, y) = 1$ und keine mit $(x, y) > 1$ besitzen.

Und zwar hat eine natürliche Zahl m eine Darstellung $m = x^2 + y^2$ mit $(x, y) = t$ nur, wenn $m = t^2 h$ und zugleich $h = u^2 + v^2$ *eigentlich* darstellbar ist, d. h. mit $(u, v) = 1$. Eigentliche Darstellungen besitzen dann alle und nur die Zahlen m, die Produkte von Primzahlen der Form $4n+1$ sind, und ihre Doppelten, *nur eigentliche* Darstellungen die quadratfreien unter ihnen, und zwar mehrere, wenn sie mehrere Primfaktoren besitzen (2^{r-1} bei r Faktoren).

Satz 47: Jede natürliche Zahl ist als Summe von vier Quadraten darstellbar.

Infolge des Wilsonschen Satzes, Formel (50), reicht es, Satz 45 „für die Primzahlen p mit lösbarer Kongruenz $z^2 \equiv -1 (p)$" zu beweisen. Und das wird nach Thue aus Satz 28 sofort folgen, weiter mit wenigen Zusätzen

Satz 48: Es ist eine Primzahl $p = x^2 + dy^2$ für $d = 1, 2, 3, 7$ darstellbar, wenn $z^2 \equiv -d \bmod p$ lösbar ist, ferner für $d = 5, 13, 37$, wenn außerdem $p = 4n+1$. Wieder sind diese p unter den ungeraden Zahlen durch eindeutige und zugleich eigentliche Darstellbarkeit ausgezeichnet.

Satz 48 werden wir zur Primzahlprüfung (§ 36) vorteilhaft verwenden. Der Beweis von Satz 47 wird ferner erleichtert, indem man zuvor beweist:

Für jede Primzahl $p = 2k + 1$ stellt sich dar

(86) $$-1 \equiv x^2 + y^2 \bmod p.$$

Beweis: Ein jeder Rest $a \equiv r^2 \bmod p$ ist Quadrat von höchstens zwei Resten; Schlußweise wie bei (61) durch Zerlegung von $x^2 - r^2$. Unter den Resten $0^2, 1^2, 2^2, \ldots, (-1)^2$ sind daher mindestens $k + 1$ Inkongruente. Bildet man nun die Paare $(0, -1), (1, -2), \ldots, (k, k)$ sämtlicher Reste mit der Summe $-1 \bmod p$, so ist entweder die Kongruenz

$$x^2 \equiv k \equiv -\tfrac{1}{2} \bmod p$$

lösbar und dann $y = x$ eine Lösung von (86), oder sonst gibt es immer noch $k + 1$ Quadratreste unter den Paaren $(0, -1)$ bis $(k - 1, -k)$, und dann muß nach dem Schubfächerprinzip ein Paar $(a, -a - 1)$ zwei Quadratreste $a \equiv x^2$, $-a - 1 \equiv y^2$ enthalten, die dann $x^2 + y^2 \equiv -1\,(p)$ liefern. (Gültig auch mod p^e.)

Satz 47 folgt jetzt so: Weil das *Produkt zweier Summen von vier Quadraten wieder* als *Summe von vier Quadraten* darstellbar ist, nämlich

(87) $$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) = A^2 + B^2 + C^2 + D^2$$

mit $$\begin{aligned} A &= ax + by + cz + dw; \quad B = ay - bx - cw + dz; \\ C &= az + bw - cx - dy; \quad D = aw - bz + cy - dx, \end{aligned}$$

wie man durch Ausrechnung bestätigt, braucht nur die Darstellbarkeit der *Primzahlen* als Summe von vier Quadraten bewiesen zu werden. Hier liefert (86) schon, daß jede Primzahl p Vielfache $mp = x^2 + y^2 + 1^2 + 0^2$ besitzt. Setzt man dabei die Lösung von (86) mit $|x|, |y| \leqq \frac{1}{2}p$ an, so ist $m \leqq \frac{1}{2}p$ und läßt sich weiter auf 1 herabdrücken: Es sei nämlich, wenn noch $m > 1$ ist, $a \equiv x\,(m)$ der kleinste Absolutrest von $x \bmod m$, ebenso b der von y. Dann ist auch

$$a^2 + b^2 + 1 \equiv 0 \bmod m,$$

also $= mm'$, wo $m' \leqq \frac{1}{2}m$. Nach (87) wird jetzt

(88) $$m^2 pm' = (ax + by + 1)^2 + (ay - bx)^2 + (a - x)^2 + (b - y)^2.$$

Dabei sind alle Summanden durch m^2 teilbar, nämlich

$$ax + by + 1 \equiv a^2 + b^2 + 1 \equiv 0\,(m),$$

ebenso $m \mid ay - bx,\ a - x,\ b - y$. Division aller Quadrate in (88) durch m^2 ergibt dann eine Darstellung von pm' als Viererquadratsumme. Entweder ist dabei schon $m' = 1$, oder es ist wieder ein kleineres pm'' darstellbar.

Der Beweis ergibt, wenn eine Lösung von (86) bekannt, einen Darstellungsalgorithmus für das p.

Beispiel: $p = 79$. $-1 \equiv 157 = 11^2 + 6^2$;
$11^2 + 6^2 + 1^2 + 0^2 = 2 \cdot 79$; $2 = 1^2 + 0^2 + 1^2 + 0^2$;
$4 \cdot 79 = 12^2 + 6^2 + 10^2 + 6^2$; $79 = 6^2 + 5^2 + 3^2 + 3^2$.

79 braucht als Zahl der Form $8n + 7$ wirklich vier Quadrate zur Darstellung, d. h. keines darf 0 sein; denn in $m = a^2 + b^2 + c^2 + d^2 \equiv 7\,(8)$ müssen drei Quadrate ungerade sein und dann je $\equiv 1\,(8)$, das vierte also $\equiv 4\,(8)$ und nicht 0. Ebenso bedarf das Vierfache einer Zahl, die vier Quadrate zur Darstellung braucht, wieder vier Quadrate, da jedes gerade sein muß, der Faktor 4 also hebbar ist. *Also brauchen alle Zahlen der Gestalt* $4^k(8n + 7)$ *vier Quadratsummanden.* Alle übrigen kommen mit drei Quadratsummanden aus; aber das ist nicht so leicht zu zeigen. Wann zwei Quadrate reichen, sagt Satz 45/46.

Beweis von Satz 45 durch 48 (ohne Verwendung des Vorigen): Für $d = 1$ sei e die kleinste Zahl mit $e^2 > p$. Dann ist nach Thue die Lösung der Kongruenz $z^2 \equiv -1\,(p)$ als Bruch $x : y$ mit $0 < x, y < e$ darstellbar, also $x^2, y^2 < p$, und es ist $x^2 + y^2 \equiv (z^2 + 1)\, y \equiv 0 \bmod p$. Also $x^2 + y^2 = mp$ und dabei $m = 1$ wegen $0 < x^2 < p$; $0 < y^2 < p$.

Ebenso erhält man für jedes d bei Lösbarkeit der Kongruenz $z^2 \equiv -d \bmod p$ aus einer Lösung $z \equiv x : y$ mit $0 < x, y < e$ eine Darstellung $x^2 + dy^2 = mp$ mit $1 \leqq m \leqq d$. Für die Fälle des Satzes 48 lassen sich dann die $m > 1$ durch Kongruenzen entweder ausschließen oder auf $m = 1$ zurückführen. Wir wollen dies nur für $d = 37$ ausführen, da aber Satz 28 in der allgemeinen Form verwenden:

Es seien e und f die kleinsten Zahlen mit $e^2 > 6p$, $f^2 > \frac{1}{6}p$ $-37 \equiv \left(\frac{x}{y}\right)^2$ mit $x < e$, $y < f$. $0 < x^2 + 37y^2 < 6p + \frac{37}{6}p$

$< 13\,p$, aber durch p teilbar. Also

$$x^2 + 37y^2 = mp \text{ mit } 1 \leqq m \leqq 12.$$

Da Heraushebung von (x, y) auf kleineres m führt, braucht nur $(x, y) = 1$ betrachtet zu werden. Also x, y nicht beide gerade und $mp \equiv 1$ oder 2 mod 4. Wegen $p = 4n + 1$ daher $m = 1, 2, 5, 6, 9$ oder 10. Da auch nicht $x \equiv y \equiv 0\,(3)$, wird $mp \equiv 1$ oder 2 mod 3, daher $m \neq 6, 9$. Da nun

$$x^2 \equiv 0, \pm 1, \quad 37y^2 \equiv 0, \pm 2 \bmod 5,$$

aber nicht $x \equiv y \equiv 0$, scheidet auch $m = 5$, 10 aus. Bleibt $m = 1$ oder 2. Aber für $m = 2$; $x \equiv y \equiv 1\,(2)$ ist

$$x^2 + 37y^2 \equiv 1 + 5 \equiv 6 \bmod 8$$

und dann $p \equiv 3 \bmod 4$.

Aus dem Beweis von Satz 48 geht ferner hervor, daß -1 nichtquadratischer Rest der Primzahlen $p = 4n + 3$ ist, weil $x^2 + y^2 = 4n + 3$ unlösbar. Ebenso folgt, daß -2 „Nichtrest" der Primzahlen $p = 8n + 5, 7$ ist und -3 Nichtrest der Primzahlen $p = 6n + 5$, weil $x^2 + 2y^2 \equiv 5, 7\,(8)$ und $x^2 + 3y^2 \equiv 5\,(6)$ unlösbar sind und auch hier im Lösbarkeitsfalle p selbst darstellbar ist.

Beweis von Satz 46: Ist $p = 4n + 3 \mid m$, so besitzt m keine eigentliche Darstellung durch $x^2 + y^2$, da sonst

$$-1 \equiv (x : y)^2 \bmod p.$$

Es muß also dann in einer Darstellung von m schon $p \mid x, y$ und $p^2 \mid m$ gelten. Wie auch $4 \mid m$ nur für $2 \mid x, y$. Es bleiben die Produkte von Primzahlen der Form $4n + 1$ und ihre Doppelten zu betrachten. Zunächst besitzen diese bestimmt Darstellungen: Ist $m = p_1 p_2 \cdots p_r$ und $p_i = x_i^2 + y_i^2 \equiv 1\,(4)$, so multipliziere man, wenn schon eine Darstellung für $p_1 \cdots p_{i-1}$ gefunden, diese nach der aus (87) durch Einsetzen von $c = d = z = w = 0$ hervorgehenden Formel (89) und erhält so schrittweise eine Darstellung für m. Für eine Faktorenzahl $r > 1$ gibt es dabei immer noch eine weitere Darstellung: Ist $p_1 \cdots p_{r-1} = a^2 + b^2$; $p_r = x^2 + y^2$, so wird

$$(89) \quad (a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 = (ay + bx)^2 + (ax - by)^2$$

bei vertauschtem x, y. Ist dabei $a > b > 0$; $x > y > 0$ ($x = y$ nur für ein $2q^2$), so ist $(ax + by)^2$ größer als alle andern Quadrate in (89) und daher beide Darstellungen verschieden. Auch für $2m$ erhält man aus ihnen durch Multiplikation mit $(1^2 + 1^2)$ zwei verschiedene Darstellungen.

Eigentlich wird hier auch für quadrathaftes m die Darstellung, wenn für die Multiplikation eines $a^2 + b^2 = t$ mit einem in ihm aufgehenden $p = x^2 + y^2$ bei $x : y \equiv a : b \bmod p$ die obere Darstellung (89) gewählt wird und $(a, b) = 1$ ist. Sind jetzt $p_1, \ldots p_s$ die verschiedenen Primteiler von m, ist P ihr Produkt und ein Teilprodukt $t = p_1 \cdots p_{i-1} = a^2 + b^2$ dargestellt, ferner $p = p_i = x^2 + y^2$, so erhält man für tp nach (89) zwei eigentliche Darstellungen mit

$$(90) \qquad \begin{array}{l} (ax + by) : (ay - bx) \equiv b : a\,(t), \equiv x : y\,(p); \\ (ay + bx) : (ax - by) \equiv b : a\,(t), \equiv y : x\,(p). \end{array}$$

Die so entstehenden 2^{s-1} Bildungen $P = A^2 + B^2$ sind daher verschieden; denn als Quotient $A : B$ oder $B : A \equiv -A : B \bmod P$ kommt hier jede der 2^s Lösungen von $z^2 \equiv -1 \bmod P$, nämlich jede Kombination der Lösungen $\pm j_i$ von

$$z^2 \equiv -1 \bmod p_i,$$

einmal vor, wie durch schrittweise Anwendung von (90) folgt. Vgl. die Verwertung dieses Ergebnisses für Primzerlegung durch Quadratsummendarstellung (§ 36)! — Jeder Darstellung $P = A^2 + B^2$ entspricht dann eine eigentliche $m = X^2 + Y^2$ mit $X : Y \equiv A : B \bmod P$.

Jetzt bleibt noch zu zeigen, daß $m = p = 4n + 1$ sowie $m = 2p$ nur eine Darstellung besitzen. Sei

$$m = x^2 + y^2 = u^2 + v^2, \quad u, v, x, y > 0$$

und u, v so angeordnet, daß $u : v \equiv x : y\,(p)$, so hat man $m^2 = (ux + vy)^2 + (uy - vx)^2$ mit $p \mid uy - vx$. Beide Summanden sind sogar durch m teilbar, weil u, v, x, y für $m = 2p$ ungerade sind. Also $ux + vy = m$; $uy - vx = 0$ und $u = x$, $v = y$ wegen $(u, v) = (x, y) = 1$. — Entsprechende Multiplikationen zeigen, daß es oben bei m nicht mehr als 2^{s-1} eigentliche Darstellungen gibt.

Damit ist Satz 46 in allen Teilen bewiesen. — Aus einer Lösung von $z^2 \equiv -1\,(p)$ die Darstellung $p = x^2 + y^2$ zu er-

halten, ist auch hier mittels (88) möglich; z. B. $22^2 \equiv -1\,(97)$; $22^2+1^2 = 97\cdot 5$; $(22^2+1^2)(2^2+1^2) = 45^2+20^2$; $97 = 9^2+4^2$.

Jedoch tritt praktisch eher die umgekehrte Aufgabe auf.

Erwähnt sei noch die Existenz einer (89) und (87) einbegreifenden Multiplikation, die ein Produkt zweier Summen von acht Quadraten wieder als Summe von acht Quadraten darstellt. Eine solche Formel gibt es jedoch nur für 2, 4 und 8 Summanden. — Als Anwendung des vorigen bringen wir

Satz 49: Es gibt je unendlich viele Primzahlen der Formen $4m+1$, $4m-1$, $3m+1$, $3m-1$.

Beweis: Ist, wie bei Satz 8, $P = 2\cdot 3\cdots q$ das Produkt der Primzahlen bis q und $q \geqq 3$, so haben $P-1$, $P+1$, P^2+1 und $3P^2+1$ nur Primteiler $> q$, und zwar hat $P-1$ wenigstens einen solchen der Form $3m-1$, weil $P-1 \equiv -1$ mod 3 ist und ein Produkt von Primzahlen $\equiv +1\,(3)$ selbst $\equiv +1$ wäre. Ebenso hat $P+1 \equiv -1\,(4)$ einen Primteiler der Form $4m-1$. Dagegen hat P^2+1 nach dem obigen nur Primteiler der Form $4m+1$ und $3P^2+1$ nur Primteiler der Form $3m+1$. Es gibt also zwischen q und $4q!^2$ sicher in jeder dieser vier arithmetischen Progressionen eine Primzahl, in jeder überhaupt daher unendlich viele.

Unabhängig vom vorigen zeigen wir schließlich

Satz 50: Eine eigentliche Darstellung $x^2+y^2=z^2$ hat zur Voraussetzung eine Darstellung

$$x = a^2-b^2,\quad y = 2ab,\quad z = a^2+b^2. \tag{91}$$

Ferner ist die Gleichung $x^4+y^4=z^2$ (außer mit $y=0$) unlösbar und damit die Fermatgleichung für den Exponenten 4.

Beweis: Da $x \smile y$ sein soll, kann man x als ungerade ansetzen; y ist dann aber gerade, da $z^2 \equiv 2\,(4)$, und dann z ungerade. Nun ist in der obigen Quadratsumme

$$x^2 = (z-y)(z+y)$$

und dabei $(z+y,\ z-y) = (z-y,\ 2y) = 1$ wegen

$$(z, 2) = (z, y) = 1.$$

Also sind $z+y=c^2$ und $z-y=d^2$ einzeln Quadrate und ungeradheitshalber noch $c = a+b$, $d = a-b$ darstellbar, woraus (91) folgt.

Soll $x^4 + y^4 = z^2$ sein, bei kleinstem z, so muß bei $y^2 = 2AB$ und $x^2 = A^2 - B^2$ das B gerade und mit $x \cup y$ auch $A \cup B$ sein und dann $A = a^2$, $B = 2b^2$. Das ergibt

$x^2 + (2b^2)^2 = a^4$ und damit $2b^2 = 2CD$, $a^2 = C^2 + D^2$.

Und wieder $C \cup D$ und dann $C = c^2$, $D = d^2$. Also: $a^2 = c^4 + d^4$; dabei $z = a^4 + 4b^4 > a^4 \geqq a$, weil mit $y > 0$ auch $b > 0$, d. h. z wäre nicht die kleinste Zahl, deren Quadrat die Summe zweier Biquadrate.

IV. Quadratische Reste.

§ 21. Zurückführung der quadratischen Kongruenz.

In diesem Abschnitt werden wir die in § 19 für die n-ten Potenzreste gestellten Hauptfragen A., B. für die quadratischen Reste behandeln; also: Welches sind die quadratischen Reste mod m? Für welche m ist eine gegebene Zahl quadratischer Rest? Oder einzeln: gegeben $r \cup m$; ist $x^2 \equiv r \bmod m$ lösbar? Für diese Fragen haben wir zwei wichtige Kriterien, das schon in § 19 erwähnte Eulersche (§ 22) und das Gaußsche Lemma (§ 23), das uns eine überraschend einfache Antwort (§ 24) geben wird: Ob r für eine Primzahl p quadratischer Rest ist, hängt nur von der Restklasse mod $4r$ ab, in der p liegt. Eine so einfache Einteilung kommt bei höheren Potenzresten nicht vor. Sie liefert ferner das Reziprozitätsgesetz der quadratischen Reste (§ 25), das über das gegenseitige quadratische Restverhalten zweier Primzahlen aussagt. Wir werden wieder alle Fragen auf den Fall des Primzahlmoduls zurückführen, sogar die allgemeine Kongruenz

(92) $$ax^2 + bx + c \equiv 0 \bmod m$$

auf den Fall $x^2 \equiv r \bmod p$; $p > 2$.

Dies führen wir sogleich aus: (92) ist gleichwertig mit $4a^2x^2 + 4abx + 4ac = (2ax + b)^2 - (b^2 - 4ac) \equiv 0 \bmod 4am$. $D = b^2 - 4ac$ heißt die Diskriminante von (92). Setzt man $2ax + b = y$, so bleibt eine reine Kongruenz

(93) $$y^2 \equiv D \bmod 4am \quad \text{mit} \quad y \equiv b \bmod 2a$$

als Nebenbedingung zu lösen. Dabei war die Erweiterung des

Modulus m mit 4 nur nötig bei geradem m, und mit a nur, soweit die Primteiler von a in m aufgehn, da sonst Bruchrechnung anwendbar.

Die Lösung von (93) läßt sich auf teilerfremden Rest zurückführen; es gilt

Satz 51 A: Die reine quadratische Kongruenz $x^2 \equiv D \bmod m$ ist für $(D, m) = d$; $d = e^2 f$, f quadratfrei; $D = dD'$, $m = dm'$ genau dann lösbar, wenn $f \cup m'$ und fD' quadratischer Rest mod m' ist.

Nämlich wenn e^2 in m und D aufgeht, so auch in x^2, also $x = ey$, und y hat noch die Kongruenz $y^2 \equiv fD' \bmod fm'$ zu erfüllen. Es muß daher f in y^2 aufgehn, quadratfreiheitshalber dann auch in y. Mit $y = fz$ bleibt $fz^2 \equiv D' \bmod m'$ zu lösen, was nach Satz 26 $(f, m') \mid (D', m') = 1$ erfordert und gleichwertig wird mit $f \cup m'$ und

(94) $\qquad y^2 \equiv fD' \bmod m'; \; y = fz. \qquad (x = efz.)$

Jetzt bleibt nur die Frage, ob ein gegebener teilerfremder Rest $a \bmod m$ quadratischer Rest oder Nichtrest.

Hier liefern die Sätze 30, 36, 41 (und 42):

Satz 51 B: Es ist a genau dann quadratischer Rest mod m, wenn a quadratischer Rest aller Primteiler von m ist und für die Fälle $4 \mid m$, $8 \mid m$ selbst $\equiv 1 \bmod 4, 8$.

Praktische Auflösung quadratischer Kongruenzen in § 38.

§ 22. Eulersches Kriterium. Legendre-Symbol.

Satz 52 (Eulersches Kriterium): Für eine Primzahl $p = 2k + 1$ ist $D^k \equiv +1, -1, 0 \bmod p$, jenachdem D quadratischer Rest, Nichtrest oder $\equiv 0 \bmod p$ ist.

$$(95) \qquad \left(\frac{D}{p}\right) = +1, \quad \left(\frac{D}{p}\right) = -1, \quad \left(\frac{D}{p}\right) = 0$$

(„D für p") ist das *Legendresche Symbol* für diese drei Arten von Restverhalten. Für das Legendre-Symbol gilt

$$(96) \qquad \left(\frac{D}{p}\right) \equiv D^k \bmod p, \quad = \left(\frac{D'}{p}\right) \text{ für } D' \equiv D. \sum_{D \equiv 0}^{p-1} \left(\frac{D}{p}\right) = 0.$$

$$(97) \qquad \left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right).$$

Ausführlich sagt (97): Das Produkt eines quadratischen Restes mit einem Nichtrest ergibt einen Nichtrest, das Produkt zweier Reste oder zweier Nichtreste aber einen Rest mod p. (Rest 0, wenn ein Faktor 0.)

Ist einer der Faktoren quadratischer Rest, so gilt das auch für jeden Modul m, da für $m \cup r \equiv x^2 \ (m)$ mit $s \equiv y^2$ auch $rs \equiv (xy)^2$ gilt und umgekehrt. Hingegen ist nicht trivial und gilt auch nur für 4 und ungerade Primpotenzmoduln, daß das Produkt zweier Nichtreste stets Rest ist.

Beweis von Satz 52 mit (96), (97): Bei Zugrundelegung eines Primitivrestes sind die quadratischen Reste die mit geradem, Nichtreste die mit ungeradem Index, woraus (97) nach Absonderung des Restes 0 folgt, ferner, daß es je k Reste und Nichtreste gibt und darum die Summenformel (96) gilt. Der Index von D^k ist $\equiv k \bmod p-1 = 2k$ für Nichtrest D und durch $2k$ teilbar für Rest D. Daraus Satz 52.

Beweis ohne Primitivrest und Fermatsatz: Man ordne die Reste $1, 2, \ldots p-1$ zu Paaren (x, y) mit $xy \equiv D \not\equiv 0 (p)$. Für Nichtrest D ist stets $y \neq x$; es gibt also k Paare, die im Produkt $(p-1)! \equiv D^k$ ergeben. Für $D \equiv (\pm z)^2$ bleiben, neben $k-1$ Paaren, z und $-z$ einzeln, und da ihr Produkt $\equiv -D$, wird hier $(p-1)! \equiv -D^k \equiv -1$, wenn man $D = 1$ einsetzt, und darum allgemein $D^k \equiv 1$ für Rest, -1 für Nichtrest. Von neuem erhält man $(p-1)! \equiv -1$ und durch Quadrierung von D^k den Fermat. (97) jetzt aus D^k, und durch Multiplikation aller Reste mit einem Nichtrest, daß die Anzahl in beiden Klassen dieselbe.

-1 ist nach dem Eulerschen Kriterium Rest für gerades k, also $p = 4n+1$, Nichtrest für $k = 2n+1$, $p = 4n+3$. Ein für Satz 48 aufschlußreiches Kriterium gewinnt man mit (97):

Satz 53: Die Kongruenz $ax^2 + cy^2 \equiv 0 \bmod p$ ist mit $x, y \not\equiv 0 (p)$ genau für $\left(\frac{a}{p}\right) = \left(\frac{-c}{p}\right)$ lösbar.

Setzt man nämlich $x = yz$, so bleibt $az^2 \equiv -c (p)$ zu lösen oder $aw \equiv -c$ durch einen quadratischen Rest w.

Z. B. kann $2x^2 + 3y^2$ nicht durch 13, 17, 19, 23 teilbar sein, wohl aber durch 5, 7, 11, 29, ..., und von diesen Primzahlen sind

wiederum die von der Form $6n + 5$, wie sich nach dem Verfahren von Satz 48 beweisen läßt, selbst durch $2x^2 + 3y^2$ darstellbar. Näheres vgl. §§ 24, 30!

§ 23. Gaußsches Lemma. Erweitertes Legendre-Symbol.

Wir bringen ein Kriterium für quadratische Reste, das sowohl für Einzelfeststellungen als besonders für den gegenseitigen Zusammenhang der quadratischen Reste wertvoll ist. Zuvor definieren wir als *Halbsystem* mod $m = 2k + 1$ ein System von Zahlen (Resten) $a_1, a_2, \ldots a_k$, das alle Reste mod m durch $0, \pm a_i$ $(i = 1, \ldots k)$ darstellt. Ein solches bilden vor allem die *untere Resthälfte* $1, 2, \ldots k$ wie die *obere* $k+1, \ldots m-1$ oder $-k, \ldots -1$.

Satz 54 (Gaußsches Lemma): Ist $p = 2k + 1$ Primzahl und a nicht durch p teilbar, ferner $a_1, \ldots a_k$ ein Halbsystem mod p und μ die Anzahl der a_i, die bei Multiplikation mit a in das entgegengesetzte Halbsystem $-a_j$ übergehn, so gilt

$$\left(\frac{a}{p}\right) = (-1)^{\mu}. \tag{99}$$

Beweis: Da ein Halbsystem von einem Paar $\pm r$ entgegengesetzter Reste $\not\equiv 0$ immer genau einen enthält, gehen zwei Halbsysteme durch Vorzeichenwechsel einzelner Reste auseinander hervor. Entsteht $c_1, \ldots c_k$ aus $a_1, \ldots a_k$ durch μ Vorzeichenwechsel, so gilt für sein Produkt

$$c_1 c_2 \cdots c_k \equiv (-1)^{\mu} a_1 a_2 \cdots a_k \bmod p. \tag{100}$$

Nun ist aber $aa_1, aa_2 \cdots aa_k$ ein Halbsystem; denn aus $aa_i \equiv \pm aa_j$ oder 0 folgte $a_i \equiv \pm a_j$ oder 0. Also

$$\left(\frac{a}{p}\right) \equiv a^k \equiv \Pi aa_i : \Pi a_i \equiv (-1)^{\mu}. \tag{101}$$

In Anlehnung an (99) definieren wir jetzt ein „Gauß-Symbol“ $\left(\frac{a}{m}\right) = (-1)^{\mu}$ für beliebig ungerades m und $a \smile m$, indem wir $1, \ldots k$ als Halbsystem wählen; μ sei dann die Anzahl der ai $(i = 1, \ldots k)$, die in die obere Resthälfte mod m fallen. Es gilt dann

Satz 55: Das Gauß-Symbol $\left(\frac{a}{m}\right) = (-1)^{\mu}$ ist

A. vom gewählten Halbsystem unabhängig,

B. ein Restcharakter $\chi(a)$ mod m, d. h.

(102) $\chi(a') = \chi(a)$ für $a' \equiv a$ und $\chi(ab) = \chi(a)\,\chi(b)$,

C. für eine Primzahl m das Legendre-Symbol.

(D. Für $a > 0$ außerdem ein Restcharakter mod $4a$.)

Beweis: C. gilt nach Satz 54, D. wird mit Satz 57 und (116) bewiesen. A. folgt so: Der Übergang von einem Halbsystem zum andern ist schrittweise durch einzelne Vorzeichenwechsel erzielbar. Es braucht daher nur gezeigt zu werden, daß μ beim Übergang vom Halbsystem $a_1, a_2, \ldots a_k$ zum Halbsystem $c_1, c_2, \ldots c_k = -a_1, +a_2, \ldots +a_k$ sich allenfalls um eine gerade Zahl ändert. Die Multiplikation der c_i mit a kann aber durch die Übergänge

(103) $\qquad c_i \to a_i \to aa_i \to ac_i$

mit $\qquad\qquad 1, \quad \mu, \quad 1$

Vorzeichenwechseln geschehn. Das sind beim Übergang von c_i zu ac_i entweder $\mu + 2$, μ oder $\mu - 2$ Wechsel.

Schließlich folgt B. so: Treten bei Multiplikation des Halbsystems a_i mit a genau $\mu(a)$ Vorzeichenwechsel (Abwanderungen ins entgegengesetzte Halbsystem) auf und $\mu(b)$ Wechsel bei Multiplikation des neuen Halbsystems $a_i a$ mit b, so $\mu(a) + \mu(b) - 2r$ (r Anzahl der Rückwechsel) bei Multiplikation der a_i mit ab. Also

(104) $$\left(\frac{ab}{m}\right) = (-1)^{\mu(ab)} = (-1)^{\mu(a)}(-1)^{\mu(b)} = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

Bemerkung: In (104) liegt, daß ein quadratischer Rest a mod m immer $\left(\frac{a}{m}\right) = +1$ hat. Es gilt jedoch nicht die Umkehrung, sobald m verschiedene Primfaktoren besitzt, und daher sagt (104) über das quadratische Restverhalten des Produktes zweier Nichtreste nichts aus. Für $m = p$ ist (97) neu bewiesen.

Wir wenden das Gaußsche Lemma sogleich auf $a = -1$ und ± 2 an und erhalten

Satz 56: Es ist -1 quadratischer Rest für die Primzahlen der Form $4n+1$, Nichtrest für $p = 4n+3$; $+2$ Rest für $p = 8n \pm 1$, Nichtrest für $8n \pm 3$; -2 Rest für $p = 8n+1$ und $8n+3$, Nichtrest für $8n+5$, 7.

Nämlich bei Multiplikation mit -1 gehn alle kReste eines Halbsystems ins entgegengesetzte über, und k ist gerade für $p = 4n+1$; multipliziert man -2 mit der unteren Resthälfte, so fallen $-2, -4, \ldots$ bis $-(k-1)$ oder $-k$ in die obere Resthälfte, eine gerade Anzahl für $k = 4n,\ 4n+1$, also $p = 8n+1, 3$. Bei $+2$ mit $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right)$ sind es gerade die übrigen Vielfachen, die in die obere Resthälfte fallen; ihre Anzahl ist $2n$ für $p = 8n \pm 1$ und $2n+1$ für $p = 8n+3,\ 5$.

Aufgabe: Man berechne ebenso, daß -3 quadratischer Rest für $p = 6n+1$, $+3$ für $p = 12n \pm 1$; $+5$ für $p = 10n \pm 1$ und -5 für $p = 20n+1, 3, 7, 9$!

§ 24. Die zweite Hauptfrage.

Satz 57 (Hauptsatz für quadratische Reste): Es ist

$$\left(\frac{a}{2a+m}\right) = \begin{cases} \left(\frac{a}{m}\right) & \text{für } a = 4n+0,1 \\ -\left(\frac{a}{m}\right) & \text{„ } a = 4n+2,3 \end{cases} > 0. \tag{105}$$

Ob a also quadratischer Rest für eine Primzahl ist, hängt nur von deren Restklasse mod $4a$ ab.

Satz 58: Für positives a gilt ferner

$$\left(\frac{a}{4at-m}\right) = \left(\frac{a}{m}\right). \tag{106}$$

Es ist danach $\left(\frac{a}{m}\right)$ für jedes m, insbesondere alle Primzahlen bekannt, wenn für die ungeraden $m \smile a$ zwischen 0 und a.

In a aufgehende Quadrate sind dabei heraushebbar, auch 4. Beispiele:

$p = 28t+$	1	3	5	9	11	13	15	17	19	23	25	27	$\}+$ Rest					
7 für p:	+	+	−	+	−	−	−	−	+	−	+	+	$\}-$ Nichtrest					
$p = 40t+$	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39		
10 für p:	+	+	−	+	−	+	−	−	−	−	+	−	+	−	+	+		
$p = 26t+$	1	3	5	7	9	11	15	17	19	21	23	25						
13 für p:	+	+	−	−	+	−	−	+	−	−	+	+						

Die Schemata müssen nach Satz 58 symmetrisch ausfallen, und es muß nach Satz 57 für $a = 7, 10$ die zweite Schemahälfte entgegengesetzt zur ersten verlaufen und daher das zweite Viertel antisymmetrisch zum ersten, das allein zu berechnen bleibt. Entweder geschieht diese Berechnung wieder nach der Lemmamethode, oder man beschränkt sich auf Legendre-Symbole und Feststellung quadratischer Reste, indem man etwa, statt 10 für 9 zu bestimmen, feststellt, daß 10 Nichtrest für 11 und wegen der Antisymmetrie dann 10 Rest für $p = 40t + 9$, z. B. $p = 89$.

Auch für die nachfolgenden Beweise der Sätze 57—60 ist zu bemerken, daß man überall mit Legendresymbolen auskommt und also den tieferliegenden Satz 55 vermeiden kann.

Beweis von Satz 57: Wir wenden das Gaußsche Lemma an und legen als Halbsystem die untere Resthälfte zugrunde. Wir haben also zum Vergleich von „a für $2a + m$“ mit „a für m“, wenn wir nicht nach dem Modul reduzieren, die zwischen 0 und $\frac{1}{2}ma$ liegenden Vielfachen von a, das sind $a, 2a, \ldots ka$, in Intervalle I_1 bis I_a je von der Länge $\frac{1}{2}m$ einzuteilen, wobei I_i von $\frac{1}{2}m(i-1)$ bis $\frac{1}{2}mi$ reicht, ebenso für $m' = 2a + m$ die Vielfachen von a bis $\frac{1}{2}m'a$ in Intervalle $I_1', \ldots I_a'$ der Länge $\frac{1}{2}m'$.

Beispiel: $a = 6$; $m = 19$, $m' = 31$.

6		**12**	**18**		24		**30**	**36**		42		**48**	**54**	
6	12	**18**	**24**	**30**	36	42	**48**	**54**	**60**	66	72	**78**	**84**	**90**

Sind nun μ_i und μ_i' die Anzahlen der Vielfachen von a in den Intervallen I_i und I_i' $(i = 1, \ldots a)$, so ist $\mu_i' = \mu_i + 1$, weil das Intervall I_i' beim selben Rest mod a beginnend wie I_i, genau a ganze Zahlen, also ein volles Restsystem mod a mehr enthält als I_i. Die Anzahlen der Vielfachen von a in den oberen Resthälften mod m und m' sind dann, wenn $a = 2r$ oder $2r + 1$,

$$\begin{aligned} \mu &= \mu_2 + \mu_4 + \cdots + \mu_{2r} \\ \mu' &= \mu_2' + \mu_4' + \cdots + \mu_{2r}' = \mu + r. \end{aligned} \tag{107}$$

Für gerades r, also $a = 4n + 0, 1$, liefert (99) somit $\left(\frac{a}{m'}\right) = \left(\frac{a}{m}\right)$, dagegen $\left(\frac{a}{m'}\right) = -\left(\frac{a}{m}\right)$ für $a = 4n + 2, 3$.

Sind demnach p und $q = 2at + p$ Primzahlen, so hat a bei geradem t denselben quadratischen Restcharakter für q wie für p, während bei ungeradem t der Rest von a mod 4 entscheidet, wie Satz 57 behauptet.

Beweis von Satz 58: Sei $m' = 4at - m > 0$ und wieder μ_i und μ_i' die Anzahlen der Vielfachen von a, die in das i-te Halbintervall mod m und m' fallen, ihre Teilsummen

$$s_i = \mu_1 + \cdots + \mu_i \quad \text{und} \quad s_i'$$

also die Anzahl der Vielfachen von a, die $\leqq \frac{1}{2} im$ und $\leqq \frac{1}{2} im'$ sind, so wird

$$(108) \quad s_i = \frac{mi}{2a}, \quad s_i' = \frac{(4at - m)i}{2a}; \quad s_i + s_i' = 2it - 1,$$

das letzte nach (9), weil $2a$ nicht in mi aufgeht. Also

$$\mu_1 + \mu_1' = 2t - 1,$$

aber $\mu_2 + \mu_2' = \mu_3 + \mu_3' = \cdots = \mu_a + \mu_a' = 2t$. Infolgedessen

$$(109) \quad \mu + \mu' = \mu_2 + \mu_2' + \mu_4 + \mu_4' + \cdots + \mu_{2r} + \mu_{2r}' = 2rt.$$

Wir betrachten noch den Fall $a < 0$, dessen Restverhalten man zwar auch aus dem von $-a$ ableiten könnte, was jedoch für $a \equiv 1$ (4) ein Umweg. Hier wird Satz 57 in der Form (105) erhalten bleiben, während (106) das Vorzeichen wechselt. Setzt man nämlich jetzt $a = -2r + 0, 1$, wobei r wieder ungerade für $a \equiv 2, 3$ (4), und teilt man die k ersten Vielfachen von a in Halbintervalle mod m auf mit μ_i Vielfachen zwischen $-\frac{1}{2} m(i-1)$ und $-\frac{1}{2} mi$, so ist jetzt $\mu = \mu_1 + \mu_3 + \cdots + \mu_{2r-1}$ die Anzahl der in die oberen Resthälften fallenden Vielfachen (r obere und r oder $r-1$ untere Halbintervalle, je nachdem $|a| = 2r$ oder $= 2r - 1$!), und es gilt für $m' = 2|a|t + m$ wieder $\mu' = \mu + rt$. Für $m' = 4|a|t - m$ gelten hier zwar ebenfalls die Beziehungen (108) mit $|a|$ statt a; jedoch wird $\mu + \mu' = \mu_1 + \mu_1' \equiv 1$ mod 2. Das gibt

Satz 59: Für negatives a gilt noch (105), aber

$$(110) \quad \left(\frac{a}{m'}\right) = -\left(\frac{a}{m}\right) \quad \text{bei} \quad m' = 4|a|t - m > 0.$$

Definiert man schließlich der ursprünglichen Bedeutung des Moduls entsprechend $\left(\frac{a}{-m}\right) = \left(\frac{a}{m}\right)$, so gilt (105) und (106) für positives a ohne Rücksicht auf das Vorzeichen des Nenners, während für negatives a ein Vorzeichenwechsel des Nenners in (105) und (110) das Vorzeichen ändert und dann $\left(\frac{a}{m}\right)$ nicht allein durch den Rest von $m \bmod 4a$ bestimmt ist.

§ 25. Das quadratische Reziprozitätsgesetz. Quadratischer Restalgorithmus.

Satz 60 (Reziprozitätsgesetz der quadratischen Reste): Für zwei ungerade positive Zahlen p und q gilt

$$(111) \qquad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{oder} \quad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right),$$

je nachdem wenigstens eine der Zahlen von der Form $4n+1$ ist oder beide von der Form $4n-1$. Auf eine Form gebracht, unter Zulassung negativer Nenner:

$$(112) \qquad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{kl+vw}$$

bei $p = 2k+1 = (-1)^v |p|$, $q = 2l+1 = (-1)^w |q| \cup p$. Wählt man die Vorzeichen so, daß $p > 0$ und $q = 4n+1$, so gilt die erste Form (111): die direkte Umkehrung.

Sind also p und q Primzahlen, und ist der quadratische Restcharakter von $q \bmod p$ bekannt, so liefert (111) den von $p \bmod q$.

Beweis (aus Satz 54, 57, 58 so geführt, daß für Primzahl-p, q nur Legendre-Symbole vorkommen und Satz 55 vermieden wird):

A. $p \equiv q\ (4)$. Bei $p - q = 4r$ wird

$$(113) \qquad \left(\frac{p}{q}\right) = \left(\frac{4r}{q}\right) = \left(\frac{r}{q}\right) = \left(\frac{r}{4r+q}\right) = \left(\frac{r}{p}\right) = \left(\frac{4r}{p}\right) = \left(\frac{-q}{p}\right) = \pm\left(\frac{q}{p}\right),$$

je nachdem $p \equiv q \equiv \pm 1\ (4)$.

B. $p \not\equiv q\,(4)$. Bei $p+q=4r$ wird

$$(114)\qquad \left(\frac{p}{q}\right)=\left(\frac{r}{q}\right)=\left(\frac{r}{4r-q}\right)=\left(\frac{r}{p}\right)=\left(\frac{q}{p}\right).$$

Damit ist das Reziprozitätsgesetz für positive p und q bewiesen. (Satz 57 und 58 werden in (113) und (114) beim Übergang von q zu $4r+q$ und $4r-q$ verwandt. Alle Nenner bleiben Primzahl.) Und es gilt (112) mit $v=w=0$.

Um (112) auch für vorzeichenbehaftete p, q zu beweisen, beachte man: beim Übergang von q zu $-q$ ändert sich l mod 2 und $\left(\frac{q}{p}\right)$ sein Vorzeichen nur für $k \not\equiv v \bmod 2$; während $\left(\frac{p}{-q}\right)=\left(\frac{p}{q}\right)$.

Beweisvariante für B.: Ohne Satz 58 zu verwenden, schließt man mit dem Gauß-Symbol aus (113) und Satz 57:

$$(115)\qquad \left(\frac{q}{p}\right)=\left(\frac{q}{p+2q}\right)=\left(\frac{p+2q}{q}\right)=\left(\frac{p}{q}\right),$$

wenn $p\equiv -1$, $q\equiv +1\,(4)$. Es wird dann $p+2q\equiv 1\,(4)$.

Aufgabe: Man beweise so wie Satz 57, daß $\left(\frac{a}{m}\right)$ für $4 \mid a$ von m nur mod a abhängt. Man braucht dann in (113) nicht erst $4r$ in r überzuführen und dann auch nicht, daß das Gauß-Symbol ein Charakter ist.

Aus dem Reziprozitätsgesetz folgt nun für das Gauß-Symbol:

$$(116)\qquad \left(\frac{a}{m}\right)=\Pi\left(\frac{a}{p}\right)\quad \text{für}\quad m=\Pi p.$$

Das ist die Jacobische Definition des quadratischen Restsymbols, die man bisweilen ergänzt durch

$$(117)\qquad \left(\frac{D}{8}\right)\ \text{oder}\ \left(\frac{D}{2}\right)=+1\ \text{für}\ D\equiv 1\,(8),\ -1\ \text{für}\ D\equiv 5\,(8).$$

Beweis von (116): Zerlegt man $a=\pm 2^e D$ so, daß $D\equiv 1\,(4)$ wird, so bleibt, da (116) für $a=-1, 2$ aus Satz 56 folgt, nur zu schließen: $\left(\frac{D}{m}\right)=\left(\frac{m}{D}\right)=\Pi\left(\frac{p}{D}\right)=\Pi\left(\frac{D}{p}\right)$.

Das Reziprozitätsgesetz liefert einen Algorithmus zur Berechnung des quadratischen Restsymbols wie folgt:

$$\left(\frac{19}{79}\right) = -\left(\frac{79}{19}\right) = -\left(\frac{3}{19}\right) = +\left(\frac{19}{3}\right) = +1.$$

$$\left(\frac{91}{281}\right) = \left(\frac{281}{91}\right) = \left(\frac{8}{91}\right) = \left(\frac{2}{91}\right) = -1.$$

$$\left(\frac{19427}{118291}\right) = -\left(\frac{19427}{1729}\right) = -\left(\frac{2}{7}\right)\left(\frac{5}{13}\right)\left(\frac{9}{19}\right) = +1.$$

Das erste Beispiel verwendet nur Legendre-Symbole, das zweite Gauß-Symbole und das dritte diese als Jacobi-Symbole.

§ 26. Der dritte Gaußsche Beweis.

Wir bringen noch den dritten, von Eisenstein vereinfachten der acht Gaußschen Beweise des quadratischen Reziprozitätsgesetzes, der wie die meisten der zahlreichen veröffentlichten Beweise unmittelbar vom Gaußschen Lemma ausgeht, ohne den Hauptsatz der quadratischen Reste zu streifen. Er ist dadurch weniger durchsichtig als der vorausgeschickte, dafür durch seine geschlossene Form, die Subtraktionen mod 2 in Additionen verwandelt, um so eleganter.

Sei wieder $p = 2k+1$, $q = 2l+1$, und betrachten wir zuerst $\left(\frac{q}{p}\right)$, indem wir wie im Lemma die k ersten Vielfachen

$$qx = \left[\frac{qx}{p}\right] p + r_x, \quad x = 1, 2, \ldots k, \tag{118}$$

bilden und dabei von den nach der Größe geordneten Resten

$$r_x = a_1, a_2, \ldots a_\lambda, p - c_1, \ldots p - c_\mu \tag{119}$$

die ersten λ in der unteren und die folgenden μ in der oberen Resthälfte liegen, so daß für das Halbsystem (119)

$$A + C = (a_1 + \cdots + a_\lambda) + (c_1 + \cdots + c_\mu) = 1 + \cdots + k = \tfrac{1}{2} k(k+1) = \tfrac{1}{8}(p^2 - 1). \tag{120}$$

Durch Summierung von (118) für alle x erhält man

$$\frac{p^2-1}{8} q = \sum_{x=1}^{k} \left[\frac{qx}{p}\right] p + A + \mu p - C, \tag{121}$$

$$\frac{p^2-1}{8} \equiv \sum \left[\frac{qx}{p}\right] + \mu + A + C \mod 2,$$

wegen (120) also $\mu \equiv \Sigma[qx:p]$. Es gilt dann nach dem Gaußschen Lemma, wenn man die gleiche Betrachtung für $\left(\frac{p}{q}\right)$ macht,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{x=1}^{k}\left[\frac{qx}{p}\right]+\sum_{y=1}^{l}\left[\frac{py}{q}\right]},$$

und es ist das Reziprozitätsgesetz (112) für $p, q > 0$ bewiesen, wenn man zeigt

$$(122)\quad \Sigma_1 + \Sigma_2 = \sum_{x=1}^{k}\left[\frac{qx}{p}\right] + \sum_{y=1}^{l}\left[\frac{py}{q}\right] \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} = kl\ (2).$$

Es gilt sogar Gleichheit in (122): Bildet man die kl Ausdrücke $qx - py$, so sind Σ_1 Ausdrücke positiv, keiner null und Σ_2 negativ; nämlich bei festem $x = 1, \ldots k$ ist $qx - py > 0$ für $y = 1, \ldots [qx:p]$, was für alle x insgesamt Σ_1 Ausdrücke gibt; ebenso $qx - py < 0$ oder $py > qx$ bei festem $y \geqq 1$ für $x \leqq [py:q]$, insgesamt Σ_2 Ausdrücke; während $py = qx$ wegen $0 < x < p$ unmöglich.

§ 27. Anwendungen. Biquadratische und kubische Reste.

Daß 2 quadratischer Rest für $p = 8n \pm 1$ und 3 Nichtrest für $p = 12n + 5$, kann zur Entscheidung, ob eine Zahl $2^m \pm 1$ Primzahl sei, beitragen. Zuerst ist

$$(123)\qquad 3^{2^{m-1}} \equiv -1 \mod 2^m + 1 \qquad (m \geqq 2)$$

notwendig und hinreichend dafür, daß $2^m + 1$ eine Primzahl. Nämlich im Primzahlfall ist m gerade, falls $m > 1$, und dann $2^m + 1 \equiv 5\,(12)$, also 3 Nichtrest, und da $\varphi(p) = 2^m$, gilt nach dem Eulerschen Kriterium (123). Umgekehrt folgt aus (123), daß $3^{2^m} \equiv +1$, und daraus mit (123), daß 3 nach wenigstens einem $p \mid 2^m + 1$ die Ordnung 2^m hat, was nur für $p \equiv 1 \mod 2^m$, also $p = 2^m + 1$ möglich.

Nach § 9 konnte $2^m + 1$ nur für $m = 2^s$ Primzahl sein. Die Untersuchung durch Teilerprobe führt hier weit: zunächst hat 2 wegen $2^{2^s} \equiv -1 \mod p \mid 2^{m+1} + 1$ die Ordnung 2^{s+1}. Also $p \equiv 1\,(2^{s+1}), \equiv 1\,(8)$ für $s > 1$ und dann 2 quadratischer Rest mod p und seine Ordnung $2^{s+1} \mid \frac{1}{2}(p-1)$; $p \equiv 1 \mod 2^{s+2}$.

So kommen für $2^{32} \pm 1$ von vornherein nur Primteiler der Form $128n + 1$ in Frage, also $p = 257, 641, 769, \ldots$, wovon 257 als Teiler von $2^{32} - 1$ ausscheidet und 641 sich gleich als Teiler erweist. Ohne Verfeinerung des Verfahrens wächst die Zahl der Proben mit s allerdings sehr stark.

Ist p und $q = 2p+1$ Primzahl, so ist $2^p - 1$ keine Primzahl, sondern durch q teilbar, wenn $p \equiv -1\,(12)$. Denn dann ist $q \equiv -1\,(8)$, also 2 qu. Rest und $2^p \equiv 1 \bmod q$, aber $q < 2^p - 1$ bei $p > 3$. $p = 11, 23, 83, \ldots$

Wir bringen nun eine Anwendung auf die Theorie der biquadratischen Reste, die im wesentlichen nur für die Primmoduln der Form $4n + 1$ Bedeutung hat. Hier gilt zunächst die einzigdastehende Tatsache:

Satz 61: Die Zahl -4 ist für alle Primzahlen der Form $4n + 1$ biquadratischer Rest, also für alle Zahlen, für die sie überhaupt quadratischer Rest ist.

Beweis: Die Zahl -1, die außer mod 2 stets von der Ordnung 2 ist, ist darum biquadratischer Rest für ein $p \equiv 1\,(8)$ und Nichtrest für $p \equiv 5\,(8)$. Dieselbe biquadratische Restverteilung gilt aber für die Zahl 4; denn 4 ist als Quadrat von 2 da biquadratischer Rest, wo 2 quadratischer Rest ist. Also ist das Produkt -4 sicher für ein $p = 8n + 1$ biquadratischer Rest, aber auch für $p = 8n + 5$; weil dann $\operatorname{ind}(-1) = 4n + 2$ und etwa $\operatorname{ind} 4 = 4m - 2$, somit $\operatorname{ind}(-4) = 4(m + n)$.

Satz 62 (Gauß): Die Zahl 2 ist biquadratischer Rest für die Primzahlen der Form $x^2 + 64y^2$ und nur für diese.

Stellt man dar: $p = 4n + 1 = a^2 + 4b^2 = a^2 + c^2$, so ist gerades b kennzeichnend für quadratischen Rest 2 (Fall $p = 8m + 1$); hier wird nun behauptet: $4 \mid b$ ist kennzeichnend für biquadratischen Rest 2.

Beweis (Dirichlet): Mit den obigen Bezeichnungen ist

$$(124) \qquad (a + c)^2 \equiv 2ac \mod p = a^2 + c^2,$$

somit bei $c \equiv ja$; $j^2 \equiv -1\,(p)$ und nach (96):

$$(125) \qquad \left(\frac{a+c}{p}\right) \equiv (a + c)^{2n} \equiv 2^n a^n c^n \equiv (2j)^n \left(\frac{a}{p}\right) \equiv 2^n j^n \bmod p,$$

weil $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = 1$ mit $p = 4n + 1 \equiv c^2 \mod a$. Ferner

$$\left(\frac{2p}{a+c}\right) = 1 \quad \text{bei} \quad 2p = (a+c)^2 + (a-c)^2. \tag{126}$$

Nun läßt sich der quadratische Charakter von 2 darstellen

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}, \tag{127}$$

da $m^2 \equiv 1(16)$ für $m \equiv \pm 1(8)$, $\equiv 9(16)$ für $m \equiv \pm 3(8)$. Dies gibt mit (126) auf (125) angewandt

$$2^n j^n \equiv \left(\frac{a+c}{p}\right) = \left(\frac{p}{a+c}\right) = \left(\frac{2}{a+c}\right) = (-1)^w = j^{2w} \tag{128}$$

mit $8w = (a+c)^2 - 1 = p - 1 + 2ac = 4n + 4ab$, also

$$2^n j^n \equiv j^{n+ab}; \quad 2^n \equiv j^{ab} \mod p. \tag{129}$$

Das Eulersche Kriterium dafür, daß 2 biquadratischer Rest ist, lautet aber $2^n \equiv 1(p)$, d. h. hier $4 \mid ab$ oder $4 \mid b$.

Im ganzen läßt sich die Theorie der biquadratischen Reste nicht so durchführen wie die der quadratischen Reste. Man kann zwar vom Eulerschen Kriterium aus noch ein Gaußsches Lemma durch Bildung von Viertelsystemen $V \mod p$ erhalten, die von je vier Resten $\pm a$, ja genau einen enthalten und durch Multiplikation mit j zyklisch auseinander hervorgehn. Es gilt dann für $p = 4n + 1$

$$a^n \equiv j^\mu \quad \text{mit} \quad \mu = x + 2y + 3z, \tag{130}$$

wenn x, y, z die Anzahlen der Reste aus V sind, die bei Multiplikation mit a in Vj, Vj^2, Vj^3 übergehn. Weil nun aber j für jedes p anders ausfällt und schon darum keine einheitliche Einteilung in Viertelsysteme gestattet, erhält man im Rationalen keine Lösung der zweiten Hauptfrage durch arithmetische Progressionen und kein Reziprozitätsgesetz. Sondern man muß hier mit Gauß in den aus der vierten Einheitswurzel i ($i^2 = -1$) gebildeten Ring Γ der Zahlen $x + iy$, x und y ganz rational, hineingehn, in dem jedes $p = 4n + 1$ zerfällt

$$p = a^2 + b^2 = (a + bi)(a - bi) \quad \text{sowie} \quad 2 = -i(1+i)^2, \tag{131}$$

während die p der Form $4n - 1$ unzerfallen bleiben. Hier hat man bei Einführung der Kongruenz durch (42) den kleinen Fermat in der Form (72), wenn φ wieder die Anzahl aller teilerfremden

Reste mod m ist (z. B. $\varphi = p - 1$ für das $a + bi$ in (131); $p^2 - 1$ für unzerfallenes p), ferner für jeden Primmodul m einen Primitivrest und das Eulersche Kriterium (84). Dies besagt, weil außer für $m = 1 + i$ immer $\varphi(m) = 4k$ ausfällt, im biquadratischen Fall

$$\alpha^k \equiv \left(\frac{\alpha}{m}\right)_4 = +1, -1 \text{ oder } \pm i \mod m, \tag{132}$$

je nachdem α in Γ biquadratischer, nur quadratischer oder nichtquadratischer Rest mod m. Zugleich ist in (132) ein biquadratisches Restsymbol $\left(\frac{\alpha}{m}\right)_4$ definiert, das $= i^\mu$ mit dem μ aus (130) wird, wenn man das Bildungsverfahren des Gaußschen Lemmas anwendet. Hier erhält man nun bei quadratischer Anordnung der Zahlen $x + yi$ feste Resteviertel mod m, die durch Multiklikation mit dem jetzt von m unabhängigen Rest i ineinander übergehen und zusammen ein reduziertes Restsystem mod m in Quadratform ergeben (vgl. Gauß, Werke, Band 2, S. 313 ff.).

Hieraus eine Lösung der zweiten Hauptfrage für biquadratische Reste durch arithmetische Progressionen im Gaußschen Ring und ein *biquadratisches Reziprozitätsgesetz* dortselbst.

Im Rationalen hat man jedoch kein biquadratisches Reziprozitätsgesetz und keine lineare Lösung der zweiten Hauptfrage; ihre Entscheidung hängt vielmehr vom Zerfall des Moduls in Γ noch ab. Sie kann aber im Zusammenhang damit aus der Darstellbarkeit durch gewisse rationalzahlige quadratische Formen getroffen werden wie oben in Satz 62.

Ähnlich verhält es sich mit der Frage nach den kubischen Resten der Moduln $p = 3n + 1$. Hier erhält man, wenn r ein Rest der Ordnung 3, mit Restedritteln T, Tr, Tr^2 und entsprechend geändertem μ ein kubisches Lemma (130) mit r statt j. Zur Lösung der zweiten Hauptfrage führt man mit Eisenstein den Ring $P = R(\varrho)$ der aus der die Gleichung $x^2 + x + 1 = 0$ befriedigenden dritten Einheitswurzel ϱ gebildeten Zahlen $a + \varrho b$ ein, in dem die

$$\begin{aligned} p = 3n + 1 = a^2 + 3b^2 &= (a + b\tau)(a - b\tau), \\ -3 = \tau^2; \qquad\qquad \tau &= 2\varrho + 1, \end{aligned} \tag{133}$$

zerfallen, während die $p = 3n - 1$ unzerfallen bleiben. Alle Primmoduln m außer τ haben dann ein $\varphi(m) = 3k$, und es entscheidet

$$\alpha^k = \left(\frac{\alpha}{m}\right)_3 = 1, \varrho, \varrho^2, \tag{134}$$

ob a kubischer Rest oder Nichtrest mod m. Endergebnis: ein kubisches Reziprozitätsgesetz in P, das im Rationalen so anwendbar:

r ist kubischer Rest für p in (133), wenn in P für $a + b\tau$. So gilt z. B. für ungerades $a + c$

$$(135) \qquad \left(\frac{2}{a + c\tau}\right) = \varrho^{ac} = 1 \text{ nur für } 3 \mid c; \qquad \text{rational:}$$

2 ist kubischer Rest gerade für die Primzahlen p der Form $a^2 + 27b^2$.

Offen blieb noch die Frage, ob in $R(i)$ und $R(\varrho)$ die Primfaktorenzerlegung bis auf Faktoren, die in 1 aufgehn, eindeutig sei. Dies bestätigt sich in $R(i)$ durch Satz 46 in Verbindung mit (89) und (90), ähnlich für $R(\varrho)$ bei den entsprechenden Folgerungen aus Satz 48; man muß nur von $a + bi$, $a + b\varrho$ erst den rationalen Faktor (a, b) abspalten, um mit eigentlichen Darstellungen wie in (131), (133) vergleichen zu können. Dasselbe gilt (vgl. nächstes Kap. bis Def. (158) !) für alle $R\left(\sqrt{D}\right)$, wo zur Diskriminante D nur eine Klasse quadratischer Formen gehört. Dagegen scheitert die eindeutige Primzahlzerlegung in $R\left(\sqrt{-5}\right)$ z. B. an der Zusatzbedingung $p = 4n + 1$ in Satz 48: es ist

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 1^2 + 5 \cdot 2^2$$

darstellbar, bei $\left(\frac{-5}{3}\right) = \left(\frac{-5}{7}\right) = 1$ und $21 \equiv 1\ (4)$, während 3 und 7, weil $\equiv -1\ (4)$ keine Zerlegung haben.

Die Prim*zahl*zerlegung ist aber für die höhere Zahlentheorie nicht so maßgebend; es kommt hauptsächlich darauf an, für die Kongruenztheorie die Zerlegung in Kongruenzen mit Restklassenkörpern zu haben, wie sie in § 16 fürs Rationale aus der eindeutigen Primzahlzerlegung folgte. Und das läßt sich für algebraische Zahlringe geeigneten Umfangs in Form einer eindeutigen Prim*ideal*zerlegung erreichen: Die Moduln bestehen hier nicht mehr aus den Vielfachen einer Zahl μ, sondern haben die allgemeinere Gestalt (13). Jedoch muß (43) halber mit α und β nicht nur $\alpha \pm \beta$, sondern auch jedes $\lambda\alpha$ (λ Ringzahl) dem Modul angehören, den man dann ein *Ideal* nennt. Vom *Primideal* verlangt man, daß sein Restklassenring nullteilerfrei ist, bei Endlichkeit nach Satz 27 also ein Körper.

Es erweist sich so jede Kongruenz nach einem Modul $\mathfrak{m}$ als gleichwertig mit einer simultanen Kongruenz nach eindeutig durch $\mathfrak{m}$ festliegenden Moduln $\mathfrak{q}_i$ („$\mathfrak{m} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$"), die ihrerseits Potenzen von Primidealen $\mathfrak{p}_i$ in dem Sinne werden, daß sich zu jedem $\mathfrak{q}$ ein π findet, für das $(\pi, \mathfrak{q}) = \mathfrak{p}$ Primideal wird ($\alpha \equiv \beta \bmod (\pi, \mathfrak{q})$ heißt: $\alpha \equiv \beta + \pi\lambda \bmod \mathfrak{q}$), und das mit $\pi^e \equiv 0(\mathfrak{q})$

jeder Zahl α eine eindeutige Darstellung

$$\alpha \equiv \alpha_0 + \alpha_1 \pi + \cdots + \alpha_{e-1} \pi^{e-1} \bmod \mathfrak{q} \quad (\text{„}\mathfrak{q} = \mathfrak{p}^e\text{“})$$

aus Zahlen eines festen Restsystems mod $\mathfrak{p}$ gibt, im Einklang mit Aufgabe C in § 16. Zerlegungen mit $e = 1$ s. § 39 Ende.

Kapitel V. Quadratische Formen.

§ 28. Darstellbarkeit. Diskriminante.

Wir haben schon in § 20 und 22 einige Fälle der Darstellbarkeit insbesondere von Primzahlen p durch quadratische Formen $ax^2 + cy^2$ betrachtet und $\left(\frac{-ac}{p}\right) = 1$ als notwendige Bedingung gefunden. Hier werden wir uns allgemeiner mit den quadratischen Formen

$$(136) \qquad F(x, y) = ax^2 + bxy + cy^2 = (a, b, c),$$

wie man sie gern durch ihre hier ganz-rationalen Koeffizienten a, b, c abkürzt, beschäftigen, insbesondere mit den durch sie darstellbaren Zahlen und deren Darstellungen. Dabei werden wir wie früher eine Zahl k als durch die Form (a, b, c) „eigentlich darstellbar“ bezeichnen, wenn $k = ax^2 + bxy + cy^2$ mit zueinander teilerfremden Zahlen x und y darstellbar ist. Es wird genügen, die durch eine gegebene Form eigentlich darstellbaren Zahlen zu betrachten, da die andern aus ihnen durch Multiplikation mit den Quadratzahlen hervorgehn: aus $k = F(x, y)$ folgt $F(tx, ty) = t^2 k$. Ebenfalls reicht es, *primitive Formen* (a, b, c) zu betrachten, d. h. Formen mit teilerfremden a, b, c; denn die durch (ta, tb, tc) darstellbaren Zahlen sind einfach die t-fachen der durch (a, b, c) darstellbaren.

Als notwendige Bedingung für die eigentliche Darstellbarkeit der Zahl m durch die primitive Form (a, b, c) werden wir in Erweiterung des oben erwähnten Falles $b = 0$ erhalten, daß die *Diskriminante*

$$(137) \qquad D = b^2 - 4ac \quad \text{von} \quad ax^2 + bxy + cy^2$$

einem Quadrat mod m kongruent ist. Ist dabei m zu D teilerfremd, also D quadratischer Rest für m, so ist umgekehrt m wenigstens durch irgendeine Form der Diskriminante D dar-

stellbar, wenn D überhaupt als Diskriminante vorkommt. Wir teilen darum alle quadratische Formen zuerst nach ihrer *Diskriminante* ein.

Diskriminantenzahlen sind die positiven und negativen Zahlen der Form $4n$ und $4n+1$. Denn $D \equiv 0$ oder $1\,(4)$ muß nach (137) erfüllt sein; dann aber braucht man nur $b \equiv D \bmod 2$ zu wählen, und man hat mit $b^2 - D = 4c$ zur Diskriminante D die Form $(1, b, c)$, die für $b = 0$ oder 1 die Hauptform heißt.

Die Quadratzahlen sind dabei die Diskriminanten der zerfallenen Formen: Ist

$$(138) \qquad ax^2 + bxy + cy^2 = (kx + ly)(mx + ny),$$

so $D = (kn + lm)^2 - 4klmn = (kn - lm)^2$, und umgekehrt folgt aus $b^2 - 4ac = q^2$ oder $4ac = (b+q)(b-q)$ mit $b + q = 2r$, $b - q = 2s$ eine Zerlegung (138) mit

$$(139) \quad k = (a, r); \quad l = (c, s); \quad m = a : (a, r); \quad n = c : (c, s).$$

Dann ist $km = a$, $ln = c$ und auch $kn + lm = b = r + s$; denn aus $rs = ac$ folgt $(a, r)\, c = (ac, rc) = (rs, rc) = r(c, s)$ und in (139) dann $kn = r$; entsprechend $lm = s$.

Da bei zerfallener Form eine lineare Darstellungsaufgabe entsteht, schließen wir Quadratdiskriminanten im folgenden von der Betrachtung aus. Von den übrigen sind am wichtigsten die *Fundamentaldiskriminanten*; das sind die, die keine echte Zerlegung $D = dq^2$, bei der d wieder Diskriminante ist, besitzen. Es darf also D durch kein ungerades Primquadrat teilbar sein, und für $4 \mid D$ muß $D \equiv 8$ oder $12 \bmod 16$ sein. Zu einer Fundamentaldiskriminante gehören nur primitive Formen, weil (aq, bq, cq) die Diskriminante $(b^2 - 4ac)\, q^2$ hat. Jede Diskriminante D steht zu genau einer Fundamentaldiskriminante d in einer Beziehung $D = dq^2$. Über die Darstellungsverwandtschaft von D und d vgl. (159).

Schließlich ist die Unterscheidung der Fälle $D > 0$ und $D < 0$ sehr wichtig. Jede Form positiver Diskriminante ist *indefinit*, d. h. sie stellt sowohl positive als negative Zahlen dar. Denn für $x \neq 0$, $y = 0$ hat $F(x, y)$ das Vorzeichen von a; für $x = -b$, $y = 2a$ aber hat

$$(140) \qquad F(x, y) = ab^2 - 2ab^2 + 4a^2c = -aD$$

das entgegengesetzte Vorzeichen, wenn $D > 0$.

Ist jedoch $D < 0$, so hat $F(x, y)$ stets das Vorzeichen von a außer für $x = y = 0$, wo $F = 0$ ist. Eine solche Form nennt man *definit*. Es ist nämlich

$$(141)\quad 4aF = (2ax + by)^2 - Dy^2 > 0 \quad \text{für} \quad D < 0,\ y \neq 0.$$

Für $D < 0$ werden wir nur die positiv definiten Formen betrachten, also a, und c, positiv annehmen. Das reicht, weil $(-a, -b, -c)$ immer $-k$ darstellt, wenn k durch (a, b, c) dargestellt wird.

Im folgenden ist „Form" stets *primitiv* und „Darstellung" stets *eigentlich* gemeint. Wir beweisen schon

Satz 63: Jede Form $F = (a, b, c)$ stellt Zahlen k dar, die zu gegebenem m teilerfremd sind.

Denn die Werte

$$F(1, 0) = a, \quad F(0, 1) = c, \quad F(1, 1) = a + b + c$$

sind bei primitivem F teilerfremd; daher gibt es zu jedem Primteiler p_i von m ein Paar x_i, y_i mit $F(x_i, y_i) \not\equiv 0 \bmod p_i$. Ist nun $x \equiv x_i$, $y \equiv y_i (p_i)$ eine Simultanlösung für alle p_i, so ist $F(x, y) \smile m$.

§ 29. Äquivalenz der Formen.

Wir wollen jetzt die Formen einer festen Diskriminante D nach den durch sie darstellbaren Zahlen ordnen. Es gilt

Satz 64 A: Zwei quadratische Formen (a, b, c) und (a', b', c') der Diskriminante D stellen dieselben Zahlen dar, wenn sie durch lineare Substitution auseinander hervorgehn.

Eine *lineare Substitution* S an der Form $F = (a, b, c)$ vornehmen bedeute dabei folgendes: man ersetze x, y in F durch

$$(142)\quad \begin{aligned} x' &= rx + vy \\ y' &= sx + wy \end{aligned}, \quad \text{vermerkt durch } S = \begin{pmatrix} r & v \\ s & w \end{pmatrix}.$$

Dann wird

$$(143)\quad F(x', y') = ax'^2 + bx'y' + cy'^2 = a'x^2 + b'xy + c'y^2$$

mit

$$(144)\quad \begin{aligned} a' &= ar^2 + brs + cs^2;\ b' = 2arv + b(rw + sv) + 2csw; \\ c' &= av^2 + bvw + cw^2;\ D' = b'^2 - 4a'c' = D(rw - sv)^2. \end{aligned}$$

Dies bestätigt man durch Ausrechnung wie auch, daß

$$(145)\qquad \begin{matrix} wx' - vy' = xj \\ -sx' + ry' = yj \end{matrix} \quad \text{mit} \quad j = rw - sv.$$

x und y sind dann auch umgekehrt ganz durch x' und y' ausdrückbar, und (a', b', c') ist zugleich mit (a, b, c) primitiv, wenn die „Substitutionsdeterminante" $j = \pm 1$ ist, und das heißt nach (144) gerade, daß D bei S ungeändert bleibt. Dann stellt aber nach (143) die aus F mit (142) hervorgehende Form

$$(146)\qquad F^S = (a, b, c)^S = (a', b', c')$$

dieselben Zahlen dar wie F. Daß auch umgekehrt zwei Formen, die dieselben Zahlen darstellen, durch lineare Substitution auseinander hervorgehn, liegt tiefer, ist aber für definite Formen aus (156) und (157) zu entnehmen.

Wir teilen jetzt die quadratischen Formen der Diskriminante D in *Klassen äquivalenter Formen* ein, indem wir zwei Formen als *äquivalent* oder *eigentlich äquivalent* bezeichnen, wenn sie mittels einer „eigentlich unimodularen" Substitution S, d. h. Determinante $j(S) = +1$, auseinander hervorgehn, und als *uneigentlich äquivalent* im Falle $j(S) = -1$.

Diese Klasseneinteilung entsteht so: Wird F durch $S = \begin{pmatrix} r & v \\ s & w \end{pmatrix}$ in $F^S = G$ übergeführt und G durch $T = \begin{pmatrix} r' & v' \\ s' & w' \end{pmatrix}$ in $G^T = H$, so F in $H = F^{ST}$ mit

$$(147)\qquad ST = \begin{pmatrix} rr' + vs' & rv' + vw' \\ sr' + ws' & sv' + ww' \end{pmatrix}; \quad j(ST) = j(S)\, j(T).$$

Und rückwärts $F = G^{S^{-1}}$ nach (145) mit

$$(148)\quad S^{-1} = \begin{pmatrix} jw & -jv \\ -js & jr \end{pmatrix}; \; SS^{-1} = E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \; j(S^{-1}) = j(S).$$

Danach wird oben H mit F (und F mit H) eigentlich äquivalent, wenn beide Formen mit G eigentlich äquivalent sind oder beide uneigentlich. Bezeichnung: $H \sim F$. Dagegen wird $H \simeq F$ (uneigentlich äquivalent), wenn $G \sim F$ und $H \simeq G$.

Obwohl es für die Darstellungsaufgabe nicht nötig wäre, zwei nur uneigentlich äquivalente Formen in verschiedene Klassen zu tun, so gibt doch die Klasseneinteilung nach eigentlicher Äqui-

valenz gerade für die Darstellung zusammengesetzter Zahlen eine bessere Übersicht. (Vgl. in § 30 die Kompositionstheorie.)

Man erhält so Paare zueinander uneigentlich äquivalenter Klassen von Formen und einzelne „zweiseitige" Klassen, deren Formen einander zugleich eigentlich und uneigentlich äquivalent sind (vgl. in § 32 die zweiseitigen Formen). Zu den zweiseitigen Klassen gehört die *Hauptklasse* mit der Hauptform $(1, .., ..)$.

Wir werden bald zeigen, daß es zu jeder Diskriminante D nur eine endliche Anzahl von Formenklassen gibt, die man kurz die *Klassenzahl* $h(D)$ von D nennt.

Die Substitution ST in (147) ist durch Aufeinanderfolge von S und T gebildet. Infolgedessen gilt das Assoziativgesetz $S(TV) = (ST)V$; selten aber ist $TS = ST$; z. B. wird

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}; \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Ferner ist $(ST)^{-1} = T^{-1}S^{-1}$ und $(S^a)^{-1} = S^{-a}$, wenn man mit S^a und S^{-a} das a-fach angewandte S und S^{-1} bezeichnet. Man bildet auch

$$\begin{pmatrix} r & v \\ s & w \end{pmatrix} + \begin{pmatrix} r' & v' \\ s' & w' \end{pmatrix} = \begin{pmatrix} r+r' & v+v' \\ s+s' & w+w' \end{pmatrix} \text{ und } -\begin{pmatrix} r & v \\ s & w \end{pmatrix} = \begin{pmatrix} -r & -v \\ -s & -w \end{pmatrix}.$$

Schließlich erhalten, wenn man der Form $F = (a, b, c)$ die Substitution $Q = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ mit der Determinante $-D$ zuordnet, die $xx' + yy' = 2F$ bei $(x, y)^Q = (x', y')$ liefert, die Transformationen (144) die Gestalt

$$(149) \qquad \begin{pmatrix} r & s \\ v & w \end{pmatrix}\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}\begin{pmatrix} r & v \\ s & w \end{pmatrix} = \begin{pmatrix} 2a' & b' \\ b' & 2c' \end{pmatrix} \text{ oder } S'Q_F = Q_G S^{-1},$$

wo $S' = \begin{pmatrix} r & s \\ v & w \end{pmatrix}$ die „Transponierte" von S und $G = F^S = (a', b', c')$.

Die Darstellungsaufgabe wird nun völlig eine Äquivalenzfrage; es gilt

Satz 64 B: Stellt die Form (a, b, c) die Zahl k dar, so gibt es eine zu (a, b, c) äquivalente Form (k, l, m).

Ist nämlich $k = ax^2 + bxy + cy^2$ mit $x \smile y$, so gibt es ein Zahlenpaar v, w mit $xw - yv = 1$. Die Substitution $S = \begin{pmatrix} x & v \\ y & w \end{pmatrix}$ führt dann (a, b, c) nach (144) in eine äquivalente Form mit dem ersten Koeffizienten k über, wie Satz 64B sagt.

Führte hier ein festes Paar v, w zur Form (k, l, m), so entsteht bei der zulässigen Ersetzung von v, w durch

$$v + xt, \quad w + yt$$

eine Form (k, l', m') mit $l' = l + 2kt$, wie (144) oder die Zerlegung

$$\begin{pmatrix} x & v + xt \\ y & w + yt \end{pmatrix} = \begin{pmatrix} x & v \\ y & w \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = S\,P(t) \tag{150}$$

ergibt. Dies sind aber auch alle aus einer festen Darstellung von k hervorgehenden Formen, eine „Schar paralleler Formen".

Es können aber auch zwei verschiedene Darstellungen von k durch $F = (a, b, c)$, etwa $k = F(x, y) = F(x', y')$, dieselbe Form $G = (k, l, m)$ hervorbringen mit $S = \begin{pmatrix} x & v \\ y & w \end{pmatrix}$ und $T = \begin{pmatrix} x' & v' \\ y' & w' \end{pmatrix}$. Aus $G = F^S = F^T$ folgt aber, daß $A = S^{-1}T$ eine „automorphe" Substitution von F ist, d. h. $F^A = F$. Kennt man die automorphen Substitutionen von F (vgl. § 32), oder die zu F selbst gehörigen Darstellungen von a durch F, so gewinnt man aus einer Darstellung von k durch F alle zur selben Formenschar (k, l', m') gehörigen. Ist diese Aufgabe gelöst, bleibt nur zu untersuchen, welche Formen

$$(k, l, m) \text{ mit } l^2 - 4km = D \text{ und } -k < l \leqq k \tag{151}$$

der Form (a, b, c) äquivalent sind, um alle Darstellungen von k durch (a, b, c) zu bekommen. Die Anzahl dieser Formen ist für eine Fundamentaldiskriminante D gleich der Anzahl der Lösungen der Kongruenz $z^2 \equiv D \bmod 4k$; für andere $D = dq^2$ sind unter den (k, l, m) in (151) noch die imprimitiven zu streichen, die jedoch nur für $(k, q) \smile 1$ auftreten. Zusammenfassend haben wir

Satz 65: Eine Zahl k ist durch irgendeine Form der Diskriminante D genau dann darstellbar, wenn die Kongruenz $l^2 \equiv D \bmod 4k$ lösbar, $l^2 = D + 4km$ und dabei $m \smile (k, l)$ ist, eine Primzahl p also sicher für $\left(\frac{D}{p}\right) = 1$, auch für $p \mid D \not\equiv 0 (p^2)$, nicht aber für $\left(\frac{D}{p}\right) = -1$.

Durch eine *bestimmte* Form $F = (a, b, c)$ der Diskriminante D ist k aber erst dann darstellbar, wenn eine der Formen (151) zu F äquivalent ist. $k = 1$ nur, wenn F zur Hauptklasse gehört. Die Gesamtheit der Darstellungen $k = F(x, y)$ entspringen den linken Zahlen x, y der Substitutionen, die die Form (a, b, c) in die verschiedenen Formen (151) überführen. Diese Formen teilen die Darstellungen von k durch F in Scharen solcher ein, die durch automorphe Substitution von F ineinander übergehn, wie umgekehrt die einzelnen Darstellungen alle zu F äquivalenten (k, l', m') nach Scharen paralleler Formen ordnen.

Dabei heißen zwei äquivalente Formen (a, b, c) und (a, b', c') *parallel*, wenn $b' \equiv b \bmod 2a$. Substitution: $P(t)$ aus (150).

Andere häufig vorkommende Äquivalenzen mit (a, b, c) sind: Die *komplementäre Form* $(c, -b, a) = (a, b, c)^L$ mit

$$L = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = MN = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

hier zusammengesetzt aus zwei Substitutionen, die einzeln zwei uneigentliche Äquivalenzen hervorbringen: die zu (a, b, c) *assoziierte Form* $(a, b, c)^M = (c, b, a)$ und die *entgegengesetzte Form* $(a, b, c)^N = (a, -b, c)$. Für die Reduktion der quadratischen Formen sind am wichtigsten die *rechts benachbarten Formen* oder *Nachbarformen*

$$(152)\quad (a,b,c)^R = (c, -b + 2ct,\ F(-1, t)); \quad R = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix} = LP,$$

also die zur komplementären Form parallelen Formen.

Beispiele für Darstellungen:

1. $x^2 + y^2 = 5$. $k = 5$, $F = (1, 0, 1)$, $D = -4$.
$z^2 \equiv -4 \bmod 20$ hat mod 10 die Lösungen ± 4. Zugeordnete Formen: $(k, l, m) = (5, 4, 1)$ und $(5, -4, 1)$. Beide stellen die Eins dar und sind daher $\sim (1, 0, 1)$ und zwar Nachbarformen. Es wird z. B. $(5, 4, 1) = (1, 0, 1)^S$ und $(5, -4, 1) = (1, 0, 1)^T$ mit $S = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ und $T = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$. Da $F^A = F$ für $A = \pm E$ und $\pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (vgl. § 32), gehören zu $(5, 4, 1)$ die aus AS hervorgehenden Darstellungen $x, y = 1, 2$; $-2, 1$; $-1, -2$; $2, -1$; zu $(5, -4, 1)$ mit vertauschtem x, y.

2. $x^2 + xy + 6y^2 = 6$. $F = (1, 1, 6)$, $D = -23$.
$z^2 \equiv 1$ (24). Lösungen: ± 1, ± 5 mod 12. Zugeordnete Formen: $(6, \pm 1, 1)$ und $(6, \pm 5, 2)$. Das letzte Paar ist zu F inäquivalent, da 2 nach (141) bei $-Dy^2 \geqq 23$ nicht durch F darstellbar. Für das Formenpaar $F^{S,T} = (6, \pm 1, 1)$ hat man $S = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ und $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, und da hier nur $\pm E$ automorph sind (vlg. § 32), die einzigen Lösungen $\pm (1, -1)$ und $\pm (0, 1)$.

3. $x^2 + xy + 7y^2 = 9$. $D = -27$. $z^2 \equiv 9 \bmod 36$.
$z \equiv 3\,(6)$; $\equiv 9, \pm 3 \bmod 18$. Primitive Formen sind $(k, l, m) = (9, \pm 3, 1)$; $l = 9$ scheidet aus. Da nur $\pm E$ automorph, bleiben nur die Lösungen $\pm (1, 1)$ und $\pm (2, -1)$.

Darstellungen durch indefinite Formen am Ende von § 31.

§ 30. Reduktion der definiten Formen. Komposition. Geschlechter.

Die Form (a, b, c) sei positiv definit, also $a, c > 0$ und $D = b^2 - 4ac < 0$. $D = -\Delta$; $\Delta = 3, 4, 7, 8, 11, 12, \ldots$.

Gelingt es, in jeder Formenklasse von D eine ausgezeichnete Form (a, b, c) festzulegen und ein Verfahren, eine gegebene Form (k, l, m) der Diskriminante D durch eigentlich unimodulare Substitution in die zu ihr äquivalente

ausgezeichnete überzuführen, zu „reduzieren", so kann man die Darstellbarkeit von k durch die Form $F = (f, g, h)$ dadurch entscheiden, daß man F und die Formen (151) reduziert: führt die Reduktion einer dieser Formen auf die ausgezeichnete Form der Klasse von F, so ist k durch F darstellbar nach Satz 65/64. (Die Anzahl der Darstellungen wird nach § 32 das Sechsfache, Vierfache, Doppelte der zu F äquivalenten Formen (151), je nachdem $\Delta = 3, 4$ oder > 4.)

(a, b, c) heiße nun eine *reduzierte Form*, wenn

(153) $\quad |b| \leqq a \leqq c. \qquad$ Folge: $\Delta = 4ac - b^2 \geqq 3b^2$.

Satz 66: A. Jede definite Form läßt sich durch eine Kette benachbarter Formen in eine reduzierte Form überführen.

B. Zwei reduzierte Formen sind einander inäquivalent, außer wenn sie einander entgegengesetzt sind und dabei in (153) einmal das Gleichheitszeichen gilt. Also es sind

(154) $\quad (a, a, c) = (a, -a, c)^P$ und $(a, b, a) = (a, -b, a)^L$

die einzigen Äquivalenzfälle reduzierter Formen.

In diesen Fällen wählt man als ausgezeichnete Form die mit positivem mittleren Koeffizienten.

Beweis von A.: Ist a die kleinste in der Klasse K darstellbare Zahl, so gibt es in ihr eine Form (a, l, m). Zu der ist genau eine Form $F = (a, b, c)$ mit $-a < b \leqq a$ parallel. Dabei ist $c \geqq a$, weil a die kleinste in K darstellbare Zahl. Also ist F reduziert.

Eine gegebene Form reduziert man nun so: Zuerst führt man sie in die parallele Form $G = (k, l, m)$ mit $-k < l \leqq m$ über; ist dann $m \geqq k$, so ist G reduziert. Sonst bilde man die Komplementärform $(m, -l, k)$ und reduziere $-l \bmod 2m$ so, daß eine Form (m, l', m') mit $-m < l' \leqq m$ entsteht. So fortfahrend bildet man eine Kette benachbarter Formen

(155) $\quad (k, l, m) \sim (m, l', m') \sim (m', l'', m'') \sim \cdots$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \sim (f, g, h) \sim \cdots,$

in der jeweils $-f < g \leqq f$, also die erste Ungleichung in (153) erfüllt ist. Da aber die Folge $k, m, m', m'', \ldots$ der äußeren

Formenzahlen nicht ständig abnehmen kann, tritt in der Kette eine Form (a, b, c) mit $a \leqq c$ auf, die dann reduziert ist.

Beweis von B. Daß außer den Parallel- und Komplementäräquivalenzen (154) keine Äquivalenz zwischen reduzierten Formen besteht, folgt so: Ist (a, b, c) reduziert, so sind die bei $x, y = 1, 0;\ 0, 1;\ 1, \pm 1$ auftretenden Werte

$$a \leqq c \leqq a - |b| + c \tag{156}$$

die kleinsten durch (a, b, c) darstellbaren Zahlen; denn für $|x| = X \geqq |y| = Y$ und $|b| = B$ wird

$$\begin{aligned} ax^2 + bxy + cy^2 &\geqq aX^2 - BXY + cY^2 \\ &\geqq (a - B)\,XY + cY^2 \geqq (a - B + c)\,Y^2 \end{aligned} \tag{157}$$

Entsprechend $\geqq (a - B + c)\,X^2$ für $Y \geqq X$. Also

$$F(x, y) \geqq a - B + c \text{ bei } X, Y \geqq 1.$$

(Die eigentlichen Darstellungen mit x oder $y = 0$ sind oben erledigt.)

Ist nun (a', b', c') ebenfalls reduziert und $\sim (a, b, c)$, so müssen die Zahlen (156) auch die kleinsten durch (a', b', c') darstellbaren sein, also sicher $a' = a$ und bei $c > a$, $c' > a'$ auch $c' = c$ und dann $|b'| = |b|$. Dasselbe gilt für $c = a$, $c' = a'$. Daß aber etwa $c = a$ und $c' > a'$, kommt nicht in Frage; denn dann wäre jetzt $c' \geqq a - B + c = 2a - B$ und $\Delta = 4a^2 - b^2 = 4a'c' - b'^2 \geqq 8a^2 - 4aB - b'^2$ und $b'^2 \geqq 4a^2 - 4aB + B^2 = (2a - B)^2 > a^2 = a'^2$. Also wäre (a', b', c') nicht reduziert.

Zu (a, b, c) kann also höchstens $(a, -b, c)$ äquivalent sein. Dies, bleibt zu beweisen, ist für $B < a < c$ nicht der Fall: es müßte bei $(a, -b, c) = (a, b, c)^S$ und $S = \begin{pmatrix} x & v \\ y & w \end{pmatrix}$ hier $a = ax^2 + bxy + cy^2$ sein; die einzigen Lösungen sind nach (157) bei $a < c$ aber $x = \pm 1$, $y = 0$, d.h. $S = \pm \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ und dann $(a, -b, c)$ parallel zu (a, b, c), also $a \mid b$ und nicht $0 < B < a$.

Damit ist Satz 66 bewiesen. Aus A. folgt mit (153):

Satz 67: Die Klassenzahl der quadratischen Formen einer negativen Diskriminante ist endlich.

Sie läßt sich durch Aufstellung aller ausgezeichneten Formen leicht bestimmen: zuerst ordne man nach $B = |b|$. Es kommt nur $B \equiv \Delta \bmod 2$ mit $3B^2 \leqq \Delta$ nach (153) in Frage und hier das Gleichheitszeichen nur für $\Delta = 3$, da es nur die Form (B, B, B) zuläßt. Also reicht $B = 1$ für ungerades $\Delta \leqq 27$; $B = 1, 3$ für $\Delta = 31$ bis 75; $B = 1, 3, 5$ für $\Delta = 79$ bis 147; ... $B = 0$ für $\Delta = 4, 8, 12$; $B = 0, 2$ für gerades $\Delta = 16$ bis 48 usw. Nun ist $\Delta + B^2 = 4n = 4ac$ beliebig so zu zerlegen, daß (153) gilt. So erhält man alle ausgezeichneten Formen (a, b, c) mit $b = B$ für (154), $b = \pm B$ sonst. Beispiele:

$D=-3$	$D=-4$	$D=-23$	$D=-39$	$D=-156$	$D=-163$
$(1,1,1)$	$(1,0,1)$	$(1,1,6)$ $(2,\pm1,3)$	$(1,1,10)$ $(2,\pm1,5)$ $(4,3,4)$	$(1,0,39)$ $(3,0,13)$ $(5,\pm2,8)$	$(1,1,41)$
$h=1$	$h=1$	$h=3$	$h=4$	$h=4$	$h=1$

sind die Klassenzahlen dieser Diskriminanten.

Die Abzählung der Klassen kann dabei ohne Aufstellung der reduzierten Formen durch Abzählung der zulässigen Teilungen $n = ac$ erfolgen, nach B summiert: $h = \Sigma H(B, n)$, H die Anzahl der ausgezeichneten Formen (a, b, c) mit $|b| = B$ und $ac = n$, d. i. bei fundamentalem $D < -4$ für $B = 0$ die halbe Anzahl der Teiler von n und für $B > 0$ der Überschuß an Teilern $> B$ über die $< B$.

Beispiel: $D = -167$. $h = H(1, 42) + H(3, 44) + H(5, 48) + H(7, 54) = 7 + 2 + 2 + 0 = 11$.

$D = -168$. $h = H(0, 42) + H(2, 43) + H(4, 46) + H(6, 51) = 4 + 0 + 0 + 0 = 4$.

(Die Differenz aufeinanderfolgender n liegt zwischen den zugehörigen B.)

Tiefer liegt folgende (zur Bestimmung der Klassenzahl nicht so geeignete) Tatsache: Für eine Primzahl $p = 8m - 1$ ist die Klassenzahl von $D = -p$ der Überschuß der quadratischen Reste in der unteren Resthälfte mod p über die Nichtreste, während für die $p = 8m + 3 > 3$ der Überschuß die dreifache Klassenzahl ergibt, der also immer positiv ist.

Hieraus gewinnt man das Vorzeichen in (51): es ist $k! \equiv (-1)^i$ für $p = 2k + 1$, wenn i die Anzahl der Nichtreste von 1 bis k, weil -1 selbst Nichtrest. Dies gibt mit obiger Tatsache

$$p = 8m - 1: \quad h + 2i = k = 4m - 1;\ i = 2m - \tfrac{1}{2}(h+1),$$
$$p = 8m + 3: \quad 3h + 2i = k = 4m + 1;\ i = 2m - \tfrac{1}{2}(3h - 1),$$
$$k! \equiv (-1)^{\frac{1}{2}(h+1)}.$$

Auch für jedes quadratfreie $d = -2k-1$ wird $\sum_{n=1}^{k} \left(\frac{d}{n}\right)$ die Klassenzahl $h(4d)$; daraus alle $h(D)$ nach (159) mit (117).

Komposition der Formen. Geschlechter. Die Kompositionstheorie, die wir schon hier erwähnen, weil sie sich an Beispielen definiter Formen genügend erläutern läßt, behandelt die Frage:

Bekannt seien die Klassen der Diskriminante D, in denen die Zahlen a und k darstellbar sind. Was lassen sich dann für Aussagen über die Klassen von D machen, die die Zahl ak darstellen?

Die Beantwortung gelingt durch eine Formenkomposition:

$$(158) \qquad (ak, l, m) = (a, l, km)\,(k, l, am)$$

soll dabei jedenfalls gelten, und dann faßt man im Einklang mit Satz 64 B die Parallelformenschar zu (ak, l, m) als Kompositum der Scharen $(a, l + 2at, \ldots)$ und $(k, l + 2kt', \ldots)$ auf. Dies gibt eine beschränkt ausführbare, aber eindeutige Scharenkomposition, deren Ursprung mit (89) zusammengeht.

Beispiele: $(2, 3, 4)\,(3, 5, 4) \sim (2, -1, 3)\,(3, -1, 2) = (6, -1, 1)$.
$(D = -23)$ $(2, -3, 4)\,(3, 5, 4) \sim (2, 5, 6)\,(3, 5, 4) = (6, 5, 2)$.
$(2, 5, 6)\,(4, 5, 3) \sim (2, -3, 4)\,(4, -3, 2) = (8, -3, 1)$.

Die Kompositionsbedingung ist bei $a \cup k$ eine erfüllbare Simultankongruenz für l. Für $(a, k) > 1$ kann sie unerfüllbar sein; z. B. ist $(2, 5, 6)$ mit $(4, 3, 2)$ nicht komponierbar. Ist sie erfüllt, so verlangt der dritte Koeffizient dazu eine Kongruenzverschärfung für l, die aber (s. o.) erfüllbar ist, wenn $(a, k) \cup D$. Es zeigt sich ferner:

Die Klasse eines Scharenkompositums ist durch die Klassen seiner Faktoren bestimmt. Dies ergibt eine *eindeutige Komposition je zweier Klassen* C und K: durch Komposition irgendeiner Form (a, b, c) aus C mit einer Form (k, l, m) aus K, bei der $k \cup a$; diese liefert Satz 63 mit 64 B. Man kann alle Klassen wie früher die Restklassen in (81) als Potenzprodukte gewisser Basisklassen $C_1, \ldots C_s$ erhalten. Ihre Eins ist die Hauptklasse mit der Form $(1, \ldots)$; sie ist das Produkt assoziierter Klassen, da $(a, b, c)(c, b, a) = (ac, b, 1)$, also das Quadrat der zweiseitigen Klassen.

Hat man durch geeignete Komposition reduzierter Formen die Klassengruppe von D auf eine Basis gebracht, so hat man die vollständige Antwort auf die ursprüngliche Frage. Stellt z. B. das

assoziierte Klassenpaar $K^{\pm 1}$ die Primzahl p dar und $L^{\pm 1}$ die Primzahl $q \neq p$, so ist pq in den Klassen $KL, K^{-1}L, KL^{-1}, K^{-1}L^{-1}$ darstellbar, die wie oben bei $D = -23$ teils zusammenfallen können. Dagegen ist p^2, da es nicht durch Komposition je einer Form aus K und K^{-1} entsteht, nur in $K^{\pm 2}$ darstellbar (bei Existenz nur zweier Formen (151) !), und auch nur für $p \nmid D$; für $p \mid D$ ist weder p mit p komponierbar noch p^2 zugleich mit p durch eine Form von D darstellbar.

Beim Übergang von D zu Dq^2, q Primzahl, gehen aus jeder Klasse eines $D < -4$ genau $q - \left(\frac{D}{q}\right)$ Klassen von Dq^2 hervor, die dieselben zu q fremden Zahlen darstellen, während für $D \geqq -4$

$$h(Dq^2) = Q \cdot h(D) \text{ mit } Q \mid q - \left(\frac{D}{q}\right) = Qn. \tag{159}$$

(Das n vgl. mit § 32 H; $n = 2$ für $D = -4$, $n = 3$ für $D = -3$.)

Die Geschlechtertheorie behandelt die Frage: Wieweit lassen sich die in den einzelnen Klassen von D darstellbaren Zahlen durch arithmetische Progressionen, in denen sie liegen, kennzeichnen? Antwort gibt

Satz 68: Teilt man die quadratischen Formenklassen so in Geschlechter ein, daß zwei Klassen genau dann demselben Geschlecht angehören, wenn die in ihnen darstellbaren Zahlen nach beliebigem Modul dieselben Restklassen durchlaufen, so besteht das 1 darstellende Geschlecht, das „Hauptgeschlecht", aus den Klassen von D, die die quadratischen Reste mod D darstellen, und das sind im Sinne der Komposition die Quadrate der Klassen.

Für ungerades $D = q_1 \cdots q_r$, primpotenzzerlegt, stellt das Hauptgeschlecht nur quadratische Reste mod D dar. Es hat D dann 2^{r-1} Geschlechter, indem die Bedingung für Darstellbarkeit von k durch eine Form von D alle 2^{r-1} Verteilungen quadratischen Restverhaltens nach den q_i, bei denen eine gerade Anzahl Nichtreste auftreten, zuläßt. Für gerades D muß man, je nach D mod 32, oft D durch $4D$ ersetzen, um im Hauptgeschlecht nur Darstellungen quadratischer Reste mod D zu haben.

Beispiele: $D = -39$ (s. o.). Zwei zweiklassige Geschlechter, weil $h = 4$ ist und D zwei Primfaktoren hat. Das Nebengeschlecht mit den Formen $(2, \pm 1, 5)$ stellt nur Zahlen k dar, die zugleich für 3 und 13 quadratischer Nichtrest sind. In beiden Geschlechtern

gilt $\left(\frac{k}{3}\right)\left(\frac{k}{13}\right)=\left(\frac{-39}{k}\right)=1$, wenn $k \cup D$, mit $\left(\frac{-39}{p}\right)=1$ für $p \mid k$. Die Klasse von $(2, 1, 5)$ hat selbst die Ordnung 4; also ist die Klassengruppe zyklisch.

$D=-168$. Vier einklassige Geschlechter. Das Hauptgeschlecht mit $(1, 0, 42)$ stellt solche k dar, die $\equiv 1$ oder 3 mod 8 sind und quadratischer Rest für 3 und 7. In den drei andern Geschlechtern ist hingegen je eine der drei Restbedingungen erfüllt. Um eine Trennung der k mod 8 zu erhalten, muß man zu $4D$ mit acht einklassigen Geschlechtern übergehn. $(13, 2, 13)$, $(12, 12, 17)$, $(8, 0, 21)$ liefern eine Basis für die Klassengruppe von $4D$, die der Basis 13, 17, 29 der darstellbaren Reste mod 168 entspricht. In der Potenzproduktdarstellung der Formen- und Restklassen durch diese Basen entsprechen sich jedoch die Exponenten immer nur mod 2.

Allein von Kongruenzangaben abhängig ist die Darstellbarkeit durch Formen der Diskriminante D wie im letzten Beispiel und Satz 48 eben nur, wenn jede Klasse von D ein Geschlecht für sich bildet, zum Quadrat also die Hauptklasse hat. Während das bei indefiniten Formen überwiegend der Fall zu sein scheint, gibt es *nur endlich viel definite einklassige Geschlechter.* Die höchstbekannte Diskriminante ist hier $-7392=-2^5 \cdot 3 \cdot 7 \cdot 11$ $(h=16)$ wie -163 die mit $h=1$.

§ 31. Reduktion der indefiniten Formen.

$D(a, b, c)=b^2-4ac>0$. $D=5, 8, 12, 13, 17, 20, 21, \ldots$ Wie schon angedeutet, werden die Klassenzahlen hier vorwiegend niedrig bleiben. Demnach wird die Auswahl ausgezeichneter Formen und die Feststellung, ob zwei vorgelegte Formen der Diskriminante D äquivalent seien, besonders im verneinenden Fall hier schwieriger sein.

Eine indefinite Form (a, b, c) heiße *reduziert*, wenn

$$0<b<f;\ |2a| \text{ und } |2c| \geqq f-b. \tag{160}$$

f sei dabei die kleinste Zahl mit $f^2>D$. Folge: $ac<0$.

Die Anzahl der reduzierten Formen ist wieder endlich; denn es ist mit $0<b<f$ auch $|ac|<D$. Wir zeigen

Satz 69: A. Jede indefinite Form läßt sich durch eine Kette benachbarter Formen in eine geschlos-

sene Kette reduzierter Formen überführen. Die Klassenzahl ist also endlich.

B. Die verschiedenen Ketten sind einander inäquivalent.

Beweis für A.: Zur Form (k, l, m) gibt es eine eindeutige Kette von Nachbarformen (a, b, c), deren mittlerer Koeffizient in seiner Restklasse mod $A = |2a|$ so gewählt ist, daß bereits $f - A \leqq b < f$ gilt, die Hälfte der Reduktionsbedingungen. Wir beweisen dann:

1. Es gibt in jeder Kette eine Form (a, b, c) mit $b > -f$.
2. Jede darauf folgende Form ist bereits reduziert.

Damit ist dann gezeigt, daß jede Form (k, l, m) mit einer reduzierten äquivalent ist und auf die erste reduzierte Form ihrer Kette nur noch reduzierte folgen. Wegen ihrer endlichen Anzahl münden sie in einen Zyklus wiederkehrender Formen ein, deren erste (a, b, c) sei. Diese folgt bei nichtreduziertem (k, l, m) zuerst auf die letzte nicht wiederkehrende Form (g', h', a) und später auf die letzte wiederkehrende (g, h, a). Da diese reduziert ist und $h' \equiv h \equiv -b \bmod A$, aber $h' \neq h$, so ist $f - A \leqq h' < f$ nicht erfüllt, also (a, b, c) die erste reduzierte Form der Kette. Die reduzierten Formen bilden alsdann die Periode.

Es bleiben also die Behauptungen 1. und 2. zu beweisen. Zum Beweis von 1. zeigen wir: Hat die Form (a, b, c) der Kette noch ein $b \leqq -f$, so gilt für die Nachbarform (c, d, e) schon $d > b + f$, und das folgt so:

Für $b \leqq -f$ ist $b^2 \geqq f^2 > D = b^2 - 4ac$, also $ac > 0$ und dann $D = b^2 - AC$, wenn man auch $|2c| = C$ setzt. Wegen $AC < b^2$ und $A \geqq f - b$, $C \geqq f - d$ wird

$$f - d \leqq C < b^2 : (f - b) < |b| = -b; \text{ also } d > b + f.$$

Nunmehr sei $b > -f$, also jetzt $b^2 < D = b^2 + AC$ bei $ac < 0$. Hieraus folgt mit $A \geqq f - b$ bereits

$$C = \frac{D - b^2}{A} < \frac{f^2 - b^2}{f - b} = f + b. \tag{161}$$

(Bei reduzierter Form gilt dann auch $A < f + b$.) Dies gibt für die Nachbarform (c, d, e) von (a, b, c) mit $C \geqq f - d$

(162) $d > -b$; $d = -b + tC$, $t > 0$; $E = A + t(b-d)$.

$$A, C, E = |2a|, |2e|, |2e|.$$

Denn mit $b < f$ wird $d > -f$ und dann $D = d^2 + CE$.

Die Behauptung 2., daß (c, d, e) eine reduzierte Form ist, folgt nun so:

$d > 0$ gilt nach (162) sicher für $C > b$, insbesondere wenn $b \leqq 0$. Ist aber $C \leqq b$, so $d \geqq f - C \geqq f - b > 0$.

$E \geqq f - d$ gilt mit $A \geqq f - b$ sicher für $t = 1$ und auch für $b \geqq d$, auch $d = f - 1$. Für $t \geqq 2$, $b < d \leqq f - 2$ ist aber $2C \leqq tC = b + d < 2d$, somit $dE > CE = D - d^2 > d(f-d)$, weil $df \leqq (f-2)f < D$.

Die Aufstellung der Perioden erfolgt leicht nach (162): $D = 89$. $(1, 9, -2) \sim (-2, 7, 5) \sim (5, 3, -4) \sim (-4, 5, 4) \sim (4, 3, -5) \sim (-5, 7, 2) \sim (2, 9, -1) \sim \cdots$.

Es folgen noch sieben Formen, deren äußere Koeffizienten aus diesen durch Umkehrung der Vorzeichen entstehen. Da nur $b = 9, 7, 5, 3, 1$ sein kann und alle (160) genügenden Zerlegungen $D - b^2 = AC$ schon in der obigen Kette vorkommen, ist die Klassenzahl $h = 1$.

$$\frac{D = 105}{h = 4} \cdot {}^1 9_6 3^4 5_5 5^4 3_6 9^1 \quad {}_1 9^6 3_4 \cdot \cdot \quad {}^3 9_2 7^7 7_2 9^3 \quad {}_3 9^2 7_7 7^2 9_3$$

$$\frac{D = 148}{h = 3} \cdot {}^1 12_1 12^1 \quad {}^3 10_4 6^7 8_3 10^4 6_7 8^3 \quad {}^3 8_7 6^4 10_3 8^7 6_4 10^3$$

$$\frac{D = 229}{h = 3} \cdot {}^1 15_1 15^1 \quad {}^3 13_5 7^9 11_3 13^5 7_9 11^3 \quad {}^3 11_9 7^5 13_3 11^9 7_5 13^3$$

Hierbei sei ${}^a b_c d^e$ die Abkürzung für $(a, b, -c) \sim (-c, d, e)$. Die Bildung der Ketten sei nochmal an der mittleren von 148 erläutert: Nachdem $b = 12$ erledigt, kommt höchstens $b = 10$ in Frage. Primitiv und reduziert sind hier nur $(\pm 3, 10, \pm 4)$. (Für $b = 10, 8, 6, \ldots$ müssen $|a|, |c| \geqq 2, 3, 4, \ldots$ sein.) Die Entwicklung erfolgt so: Für $|c| \geqq b$ wird $d = C - b$ („Spiegelung von b an $|c|$“); für $|c| < b$ ist b am nächsthöheren Vielfachen von c zu spiegeln, wenn das ein $d < f$ ergibt, sonst am nächstniederen. Das e liefert (162).

Besonderes an obigen Beispielen: $D = 105$ hat vier einklassige Geschlechter. Da -1 nichtquadratischer Rest für D, ist sie nicht in der Hauptklasse darstellbar und kommt erst in der zweiten Kette vor. — Die drei Klassen von $D = 148$ gehen aus der einen von $D = 37$ durch Substitutionen der Determinante 2 hervor (vgl. (159) und § 32 H.). $D = 229$ ist die kleinste positive Primdiskriminante mit mehreren Klassen. Vermutlich gibt es unendlich viele mit der Klassenzahl 1.

Die Inäquivalenz der verschiedenen Ketten (Satz 69 B.) folgt nun aus dem schärferen

Satz 70 (Mertens): Sind F und $G = F^S$ zwei reduzierte indefinite Formen, so ist die eine der Substitutionen $\pm S^{\pm 1}$ das Produkt aufeinanderfolgender Nachbarsubstitutionen der von F oder G aus gebildeten Kette, der dann also auch die andere Form angehört.

Ist insbesondere $G = F$, also S automorph, so gilt

$$\pm S^{\pm 1} = A^a \quad \text{oder} \quad S = \pm A^{\pm a}, \tag{163}$$

wo A das Produkt eines von F aus genommenen vollen Umlaufs von Nachbarsubstitutionen ist und a die Anzahl der Umläufe. Die Darstellung (163) ist eindeutig; es gibt also unendlich viele Automorphe.

Beweis: Sei $F = (a, b, c)$, $G = (a', b', c')$ und $S = \begin{pmatrix} r & v \\ s & w \end{pmatrix} \neq E$, $F_1 = (c, d, e) = F^R$ der Kettennachbar von F, somit

$$S = RT = \begin{pmatrix} 0 & -1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} s' & w' \\ -r & -v \end{pmatrix} \quad \text{mit} \quad \begin{matrix} s' = q_1 r + s \\ w' = q_1 v + w \end{matrix}, \tag{164}$$

und $G = (c, d, e)^T$. Es wird genügen zu zeigen, daß bei rechter Wahl zwischen S und S^{-1} die von F ausgehenden Nachbarsubstitutionen $R = R(q_1), R(q_2), \ldots$ in (164) rechts einen Divisionsalgorithmus erzeugen. Wir dürfen dabei $a, a' > 0$, also $c, c' < 0$ annehmen; denn die andern Vorzeichenverteilungen kommen bei den Nachbarformen von F und G vor, und ein Nachbaraustausch macht für Satz 70 nichts aus. Bei dieser Vorzeichenverteilung ist $rsvw \neq 0$, nämlich G zu

F weder benachbart noch parallel. Außerdem gilt $rw > 0$; denn aus (144) folgt unter Verwendung von $rw - sv = 1$

$$a'vw - c'rs = arv - csw. \tag{165}$$

Wegen $rsvw > 0$ und $a'c', ac < 0$ hat $-csw$ das Vorzeichen von arv, ebenfalls dann $a'vw$ und $-c'rs$. Also $(rv)(vw) > 0$ und $rw > 0, sv > 0$. Unter den $\pm S^{\pm 1} = \pm \begin{pmatrix} r & v \\ s & w \end{pmatrix}, \pm \begin{pmatrix} w & -v \\ -s & r \end{pmatrix}$ hat dann genau eine lauter positive Zahlen. Trifft dies für S zu, so behaupten wir, daß S oder $-S$ das geforderte Produkt wird. Gilt nämlich

$$0 \leqq s' < r \leqq s \text{ und } 0 < w' \leqq v < w, \tag{166}$$

wie wir unten zeigen, so wird G für $s' = 0$ zu F_1 benachbart und als reduzierte Form der Kettennachbar F_2 zu F_1, somit $v = q_2$ in $T = \begin{pmatrix} 0 & 1 \\ -1 & -v \end{pmatrix}$, weil sonst G nur parallel zu F_2 würde, für $s' > 0$ aber

$$S = -R(q_1)\,R(q_2)\,S' \text{ mit } S' = \begin{pmatrix} r' & v' \\ s' & w' \end{pmatrix} \text{ und } G = F_2 S'.$$

Dann gilt, weil schon $s', w' > 0$, für S' auch $0 < r' \leqq s'$, $0 < v' < w'$ und damit

$$0 < r' < r, \quad 0 < s' < s, \quad 0 < v' < v, \quad 0 < w' < w,$$

und es folgt eine Darstellung $S = (-1)^m R(q_1) \cdots R(q_{2m})$.

Bleibt (166) zu zeigen: Mit $v \geqq w$ wäre $c' \geqq (a + b + c)w^2 \geqq a + b - |c| \geqq 0$ nach (160), (161). Ebenso wäre $a' = er^2 - drs' - |c|s'^2 \leqq (e - d - |c|)s'^2 \leqq 0$ für $s' \geqq r$. Also $v < w$, $s' < r$ und damit $r \leqq s$, $w' \leqq v$ wegen $rw - sv = rw' - s'v = 1$. Hiernach sind auch mit $r, v > 0$ von den restlichen Behauptungen $s' \geqq 0$, $w' > 0$ *beide* oder *keine* erfüllt.

Setzt man schließlich (165) für F_1 statt F an, so wird $a'vw' - c'rs' = erv - cs'w' > 0$, weil $-c$, $erv > 0$ und $s'w' \geqq 0$, also $a'vw' > c'rs'$ und dann $s' \geqq 0, w' > 0$; denn sonst wäre $a'vw' \leqq 0 < c'rs'$.

Damit ist die Inäquivalenz der Ketten durch Satz 70 bewiesen, und es besitzt F auch keine andern Automorphen

als die in (163), weil ein $R(q_i)$-Produkt erst dann wieder zu F zurückführt, wenn es aus vollen Zyklen besteht. Da

(167) $R(q_1)\cdots R(q_n) = \begin{pmatrix} r_{n-1} & r_n \\ s_{n-1} & s_n \end{pmatrix}$ mit $\begin{matrix} r_n = r_{n-1}q_n - r_{n-2} \\ s_n = s_{n-1}q_n - s_{n-2} \end{matrix}$

bei $r_0 = 0$, $s_0 = 1$; $r_i, s_i < 0$ für $i \equiv 1,2\,(4)$, sonst > 0, ferner

(168) $\left[\frac{|s_i|}{|r_i|}\right] = |q_1|$, $\left[\frac{|r_n|}{|r_{n-1}|}\right] = \left[\frac{|s_n|}{|s_{n-1}|}\right] = |q_n|$,

wie aus (167) rechts unter Vorzeichengleichheit der Summanden folgt, so ist immer $s_n > r_{n-1}$ und nur eins der $\pm S^{\pm 1}$ ein $R(q_i)$-Produkt. Ebenso wird nie $A^n = E$, und darum ist die Anzahl der Automorphen unendlich.

Mit $f - C \leqq d = -b + C\,|\,q_1| < f$, $F_1 = (c, d, e)$, wird $|q_1| = \left[\frac{b+f-1}{C}\right] = \left[\frac{b+\sqrt{D}}{-2c}\right]$ im geordneten Ring der Zahlen $x + y\sqrt{D}$ (§ 32). Die Entwicklung der „zu $F = (a, b, c)$ gehörigen Wurzel" $\frac{2a}{-b+\sqrt{D}} = \frac{b+\sqrt{D}}{-2c} = |q_1| + 1 : \frac{-2c}{-d+\sqrt{D}}$ in einen Kettenbruch (vgl. Perron, Kettenbrüche) hat dann die periodischen Nenner $|q_n|$ und die Näherungsbrüche $|s_n| : |r_n|$ nach (168).

Die Reduktion der Formen liefert ein brauchbares Verfahren zur Gewinnung von Darstellungen. Beispiele:

$F(x, y) = x^2 + 9xy - 2y^2 = -1;\ 2;\ 10.$ $D = 89$ (s. o.).

Reduktion: $(-1, 9, 2) = (1, 9, -2)^S$ mit $S = \begin{pmatrix} r_6 & r_7 \\ s_6 & s_7 \end{pmatrix}$ nach (168) und

i	1	2	3	4	5	6	7	13	14
r_i	-1	-1	2	3	-5	-23	212	-23001	-212000
s_i	-4	-5	9	14	-23	-106	977	-106000	-977001

Hieraus $F(23, 106) = -1$ und die Darstellungen $F(5, 23) = F(212, 977) = 2$, die zu $(2, 9, -1)$ und $(2, 7, -5)$ gehören. Aus diesen erhält man alle Darstellungen mit $x > 0$ durch wiederholte Bildung $r_{13}x + r_{14}y = x'$; $s_{13}x + s_{14}y = y'$ und rückwärts mit $A^{-1} = \begin{pmatrix} s_{14} & -r_{14} \\ -s_{13} & r_{13} \end{pmatrix}$. Z. B. geht mit A^{-1} aus

der Lösung $x = 212$, $y = 977$ für 2 die Lösung $x' = r_7 = 212$, $y' = r_6 = -23$ hervor, am einfachsten so: es geht $(1, 9, -2)$ in $(-1, 9, 2)$ rückwärts durch $R(q_{14})^{-1} \cdots R(q_8)^{-1} = \begin{pmatrix} s_7 & r_7 \\ s_6 & r_6 \end{pmatrix}$ über, weil allgemein $(-a, b, -c)$ bei $\begin{pmatrix} r & -v \\ -s & w \end{pmatrix}$ in $(-k, l, -m)$ übergeht und umgekehrt bei $\begin{pmatrix} w & v \\ s & r \end{pmatrix}$, wenn (a, b, c) bei $\begin{pmatrix} r & v \\ s & w \end{pmatrix}$ in (k, l, m) übergeht; wie auch oben zur Berechnung von A aus S vorteilhaft verwandt wird.

Die Darstellungen von 10 ordnen sich nach den halb reduzierten Formen $(10, \pm 3, -2)$ und $(10, \pm 7, -1)$ in vier Scharen. Zu $G = (10, +3, -2) \sim (-2, 9, 1) \sim (1, \ldots) = G^{R(-3)R(9)}$, also $G = F^S$; $S = \begin{pmatrix} 28 & 9 \\ -3 & 1 \end{pmatrix}$, gehört die kleinste Darstellung $x = 28$, $y = -3$, zu $(10, -3, -2) = (1, 9, -2)^{P'(3)}$, $P'(q) = \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}$, die Darstellung $x = 1$, $y = 3$, zu G, $H = (10, \pm 7, -1)$, $G = (2, 9, -1)^{P'(1)}$, $H = (2, 9, -1)^{P'(8)} = F^{S_0 P'(8)}$ die Darstellungen $x = 5 + 1 \cdot 23 = 28$, $y = 23 + 1 \cdot 106 = 129$ und $x = 5 + 8 \cdot 23 = 189$, $y = 23 + 8 \cdot 106 = 871$. (Letzte Lösung geht bei A^{-1} in $x = 1189$, $y = -129$ über.)

$F(x, y) = 11x^2 + 19xy + 3y^2 = 25$. $D = 229$. Von den Formen $G = (25, -23, \ldots)$ und $H = (25, -27, \ldots) \sim F$ ist hier nur $G \sim F$. Es gibt darum nur eine Schar von Lösungen. Zu ihrer Bestimmung führen wir F vorwärts und G rückwärts in die Kette:

$$(11, 19, 3) \sim (3, 11, -9) \sim (-9, 7, 5) \sim (5, -27, 25) \sim (25, -23, \ldots)$$

$$R(5) \cdot R(-1) \cdot R(-2) = \begin{pmatrix} 1 & -1 \\ -6 & 7 \end{pmatrix}$$

Hieraus die Lösung $x = 1$, $y = -7$, nach einmaligem Rechtsumlauf $x = 286$, $y = -1627$; linksherum $x = 59$, $y = -38$.

Die Lösungen liegen hier dichter als oben; automorph für F ist hier $\begin{pmatrix} -29 & -45 \\ 165 & 256 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 31 & 135 \\ 45 & 196 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix}$, dabei

$\begin{pmatrix} 31 & 135 \\ 45 & 196 \end{pmatrix} = R(-1)\,R(2)\,R(-4)\cdot R(1)\,R(-2)\,R(4)$ der Substitutionszyklus der mit $(3, 11, -9)$ beginnenden Kette (s. o. $D = 229$).

§ 32. Automorphe Substitutionen. Die Pellsche Gleichung.

Durch Satz 70 war die Frage nach sämtlichen Darstellungen einer Zahl k durch eine indefinite Form (a, b, c) schon gelöst, und zwar gab die Kettenentwicklung der Formen ein Verfahren zur Gewinnung der Darstellungen. Auch im definiten Fall konnte man aus (157) die Anzahl der Darstellungen der kleinsten in einer Klasse darstellbaren Zahl, sechs bei $(1, \pm 1, 1)$, vier bei $(a, \pm b, a)$ und zwei bei den andern reduzierten Formen, gewinnen und daraus die Anzahl der automorphen Substitutionen, wobei zu beachten, daß zu (a, b, a) bei $a > 1$ zwei Formen (151) gehören, somit nur zwei Automorphe vorhanden sind. Ferner gilt: Ist A für F automorph und $F^S = G$, so ist $S^{-1}AS = A^S$ eine automorphe Substitution für G.

Zwischen den Automorphen aller Formen einer Diskriminante D besteht folgender Zusammenhang: Für $F^S = F$ mit $S = \begin{pmatrix} r & v \\ s & w \end{pmatrix}$, $rw - sv = +1$, gilt nach (149)

$$\begin{pmatrix} r & s \\ v & w \end{pmatrix}\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}\begin{pmatrix} w-v \\ -s \quad r \end{pmatrix}, \tag{169}$$

einzeln: $bs = a(w - r)$; $-bv = c(w - r)$; $cs = -av$. Also $a \mid s$ wegen $a \mid bs, cs$ und $a \smile (b, c)$. Mit $s = au$, $w + r = t$ wird

$$r = \tfrac{1}{2}(t - bu),\ s = au,\ v = -cu,\ w = \tfrac{1}{2}(t + bu); \tag{170}$$

$$4(rw - sv) = t^2 - Du^2 = 4. \tag{171}$$

Dies ist die „Pellsche Gleichung", die nach Satz 70 unendlich viele Lösungen für $D > 0$ besitzt. (Den klassischen Dirichletschen Beweis s. u.) Für $D < -4$ hat sie nur die trivialen Lösungen $t = \pm 2$, $u = 0$, zu der nach (170) die automorphen Substitutionen $\pm E$ gehören. Für $D = -4$ kommen noch

$t = 0$, $u = \pm 1$ und für $D = -3$ als dritte bis sechste Lösung $|t| = |u| = 1$ hinzu. Für $D > 0$ ist die zu einer von (a, b, c) ausgehenden Periode gehörige Lösung von (171) eine mit kleinstem $|u|$, also $(\pm T, \pm U)$, wo T, U die kleinste positive Lösung der Pellschen Gleichung; denn bei Potenzierung der Substitution (170) vergrößern sich t, u; es gelten die Rekursionsformeln

$$(172)\quad \begin{matrix} T_n = TT_{n-1} - T_{n-2}. & T_0 = 2, T_1 = T, T_2 = T^2 - 2. \\ U_n = TU_{n-1} - U_{n-2}. & U_0 = 0, U_1 = U, U_2 = TU. \end{matrix}$$

$T_3 = T^3 - 3T$; $U_3 = (T^2 - 1)U, \ldots$ Hierbei sind T_n, U_n die durch Bildung von A^n in (163) entstehenden positiv genommenen Lösungen von (171). $T_n, -U_n$ ergibt die zur Substitution von T_n, U_n inverse.

Auch für irgendeine Lösung t, u und die Potenzen der zugehörigen Automorphen A gelten die entsprechenden Rekursionen (172) und folgen sie durch gliedweise Addition in (170) mit

$$A^n + A^{n-2} = A^{n-1}(A + A^{-1}) = t \cdot A^{n-1}.$$ Also:

Satz 71: Die Lösungen der Pellschen Gleichung (171) vermitteln durch (170) die eigentlich automorphen Substitutionen aller quadratischen Formen der Diskriminante D. Ihre Anzahl ist für $D > 0$ unendlich, und es gehen die positiven Lösungen $t, u > 0$ aus ihrer kleinsten durch (172) hervor.

Betrachten wir auch die Formenklassen mit uneigentlich automorphen Substitutionen! Wir zeigen, daß jede solche Klasse eine *zweiseitige Form* (k, kl, m), d. h. eine zu ihrer entgegengesetzten parallele Form, enthält, für die $U = \begin{pmatrix} 1 & l \\ 0 & -1 \end{pmatrix}$ automorph ist. Ist nämlich $S = \begin{pmatrix} r & v \\ s & w \end{pmatrix}$ mit $rw - sv = -1$ automorph für (a, b, c), so muß (169) rechts mit $\begin{pmatrix} -w & v \\ s & -r \end{pmatrix}$ gelten und die auch hinreichenden Bedingungen

$$(173)\qquad w = -r,\ av = br + cs \qquad (r^2 + sv = 1).$$

Eine Substitution T, die (a, b, c) in eine zweiseitige Form überführt, die also S in die Gestalt U transformiert, braucht, wie der Ansatz $ST = TU$ oder

$$\begin{pmatrix} r & v \\ s & w \end{pmatrix}\begin{pmatrix} x & \cdot \\ y & \cdot \end{pmatrix} = \begin{pmatrix} x & \cdot \\ y & \cdot \end{pmatrix}\begin{pmatrix} 1 & \cdot \\ 0 & -1 \end{pmatrix}$$

ergibt, nur die wegen $r^2 + sv = 1$ verträglichen Bedingungen

$$(174) \qquad y : x = -(r-1) : v = s : (r+1) \quad \text{mit} \quad x \smile y$$

zu erfüllen; dann erhält U die vorderen Zahlen 1, 0 und damit -1 als vierte. Weiter folgt $k \mid D = k^2 l^2 - 4km$, und diese Schlüsse gelten bei Fundamental-D für die darstellbaren Teiler $(k \neq 4n)$ auch rückwärts, also

Satz 72: Alle zweiseitigen Klassen stellen Diskriminantenteiler dar, für eine Fundamentaldiskriminante auch nur die zweiseitigen.

Genau sind es für $D < 0$ immer ein Paar Diskriminantenteiler mit dem Produkt $-D$, für $D > 0$ zwei Paare, und zwar in der Hauptklasse oft ± 1, $\pm D$, öfters $1, P, -Q, -D$ mit $PQ = D$. Dies führt zur wichtigen Frage:

Wann ist -1 in der Hauptklasse darstellbar? Oder: Welches sind die Bedingungen für die Lösbarkeit der „Nicht-Pellschen" Gleichung

$$(175) \qquad t^2 - Du^2 = -4?$$

(Der Zusammenhang beider Fragen ist allgemein: Ist k in der Hauptklasse darstellbar, also $k = x^2 + bxy + cy^2$ mit $D = b^2 - 4c$, so wird $(2x + by)^2 - Dy^2 = 4k$ und umgekehrt.)

Ist (175) lösbar, und setzt man die Lösungen in (170) ein, so haben die Substitutionen, die die Form (a, b, c) in

$$(-a, b, -c)$$

überführen, die Gestalt $V = \begin{pmatrix} -r & v \\ -s & w \end{pmatrix}$. Denn es ist hier rechts in (169) a, c durch $-a, -c$ zu ersetzen, und dann bleibt bei beiderseitiger Ersetzung von r, s durch $-r, -s$ alles weitere richtig. $W = \begin{pmatrix} -r & -v \\ s & w \end{pmatrix}$ führt dann $(-a, b, -c)$ in (a, b, c) über, und für kleinstes positives t, u werden $\pm VWVWV \ldots$,

$WVWV\ldots$ bei reduziertem F, G die Substitutionen, die F und G in der Kette nach rechts abwechselnd ineinander und in sich überführen. Die zugehörigen Werte $t_n, u_n (t_1 = t, u_1 = u)$ erfüllen abwechselnd (175) und (171) und haben bei

$$SVW - S = SV(W - V^{-1}) = SV \begin{pmatrix} -t & 0 \\ 0 & t \end{pmatrix},$$

wie man durch Einsetzen von $S = E, W, VW, WVW, \ldots$ und Koeffizientenvergleich erhält, die Rekursionsformeln

$$(176) \quad \begin{matrix} t_n = t\,t_{n-1} + t_{n-2}. & t_2 = t^2 + 2;\ t_3 = t^3 + 3t; \ldots \\ u_n = tu_{n-1} + u_{n-2}. & u_2 = tu;\ u_3 = (t^2 + 1)\,u; \ldots \end{matrix}$$

$t_1^2 - Du_1^2 = t_3^2 - Du_3^2 = \cdots = -4$. $t_{2m}, u_{2m} = T_m, U_m$ in (172).

Beispiele:	$D =$	5	8	13
$t =$	1, 3, 4, 7, 11, 18, 29 47	2, 6, 14, 34	3, 11, 36	
$u =$	1, 1, 2, 3, 5, 8, 13, 21	1, 2, 5, 12,	1, 3, 10	

$D =$	21	73	89	136	145
$t =$	$-, 5, -, 23$	2136, 4562498	1000, 1000002	$-, 70$	24, 578
$u =$	$-, 1, -, 5$	250, 534000	106, 106000	$-, 6$	2, 48

(Aufeinanderfolgende Lösungen von (175) und (171); diese durch Striche getrennt, wo (175) unlösbar.)

Klar ist, daß $t^2 - Du^2 = -4$ für $D = q^2 + 1, q^2 + 4$ lösbar ist und unlösbar für $D = q^2 - 1, q^2 - 4$, ferner, wenn D einen Primfaktor der Form $4n - 1$ hat. Weiter gilt

Satz 73: Ist D Primzahl, so ist (175) lösbar.

Ist nämlich T, U die kleinste Lösung von (171), $D = p \equiv 1\,(4)$, so ist T wegen $T^2 - 4 = DU^2 \not\equiv -4\,(16)$ nicht durch 4 teilbar. Es ist dann $(T + 2, T - 2) = 1$ oder 4 und damit

$$(177) \qquad T - 2 = t^2,\ T + 2 = pu^2 \quad \text{mit} \quad tu = U$$

oder umgekehrt $p \mid T - 2$, was aber eine kleinere Lösung von (171) lieferte. Also gilt (177) und $t^2 - pu^2 = -4$.

Allgemein geht aus dieser Überlegung eine Darstellung $Pt^2 - Qu^2 = 4$ hervor mit $PQ = D$, aus der das in der Hauptklasse darstellbare Teilerpaar $P, -Q \not\equiv 1, -D$ entspringt. Für $D = pq$, Produkt zweier Primzahlen der Form $4n + 1$, die zueinander quadratischer Nichtrest sind, kann dies nur das Paar $pq, -1$

sein, und (175) ist lösbar (auch wenn p und q zwar quadratische, aber nicht biquadratische Reste zueinander sind, dagegen nicht lösbar, wenn q für p biquadratischer Rest, aber nicht umgekehrt; was jedoch tiefer liegt).

Zum Abschluß bringen wir unter Einführung des nach den Regeln 3. und 7. des § 3 geordneten Körpers $R(\sqrt{D})$ den Dirichletschen Beweis des Satzes 71 in der Form:

Satz 74: Die Pellsche Gleichung $t^2 - Du^2 = 4$ ist für jedes $D > 0, \neq q^2$ lösbar. Ordnet man der Lösung t, u die „Pellsche Einheit" $\varepsilon = \frac{1}{2}(t + u\sqrt{D})$ zu, die

$$\varepsilon(t, u) \cdot \varepsilon(t, -u) = 1$$

erfüllt, so gehen alle Lösungen aus der Einheit $E = \varepsilon(T, U)$ der kleinsten Lösung durch $\varepsilon = \pm E^{\pm a}$ eindeutig hervor, wo a alle natürlichen Zahlen durchläuft.

Beweis: A. Zu jedem positiv-ganzen m gibt es Paare ganzer teilerfremder x, y mit

$$|x - y\sqrt{D}| < \frac{1}{m} \quad \text{und} \quad 0 < y \leqq m. \tag{178}$$

Wählt man nämlich zu jedem $y = 0, 1, \ldots m$ ein $x(y)$ so, daß $0 \leqq z = x(y) - y\sqrt{D} < 1$, so hat man $m + 1$ verschiedene $z(y)$, von denen nach dem Schubfächerprinzip mindestens zwei in eins der m Intervalle $0 \leqq z < \frac{1}{m}$ bis $\frac{m-1}{m} \leqq z < 1$ fallen müssen. Die Differenz zweier solcher z hat aber die Eigenschaft (178), auch nach Division durch (x, y).

B. Es gibt unendlich viele Paare x, y mit

$$|x - y\sqrt{D}| < \frac{1}{y}. \tag{179}$$

Man wähle nämlich $m_1, y_1, m_2, y_2, \ldots$ nacheinander so, daß

$$\frac{1}{m_1} > |x_1 - y_1\sqrt{D}| > \frac{1}{m_2} > |x_2 - y_2\sqrt{D}| > \frac{1}{m_3} > |x_3 - y_3\sqrt{D}| > \cdots.$$

Dies ist nach A. mit $y_i \leqq m_i$ möglich, wie (179) fordert.

C. Für die unendlich vielen (179) erfüllenden Paare $x \cup y$ ist

$$|x^2 - Dy^2| = |x - y\sqrt{D}|\,|x + y\sqrt{D}| < \frac{1}{y}\left(\frac{1}{y} + 2y\sqrt{D}\right) < 1 + 2\sqrt{D}.$$

Unter dieser Absolutgrenze ist dann wenigstens eine Zahl $k = x^2 - Dy^2$ unendlich oft eigentlich darstellbar.

D. Hierunter gibt es sicher zwei Darstellungen x, y und x', y' mit $x' \equiv x, y' \equiv y \mod k$. Bildet man $(x + y\sqrt{D})(x' - y'\sqrt{D}) = v + w\sqrt{D}$, so hat man

$$(180) \quad \begin{matrix} v = xx' - yy'D \equiv x^2 - Dy^2 \equiv 0 \\ w = yx' - xy' \quad \equiv 0 \end{matrix} \mod k; \qquad \begin{matrix} v = kr, \\ w = ks, \end{matrix}$$

aber $w \neq 0$, weil beides eigentliche Darstellungen. Daraus

$$(181) \quad v^2 - Dw^2 = (x^2 - Dy^2)(x'^2 - Dy'^2) = k^2; \quad r^2 - Ds^2 = 1.$$

Man hat also schon eine gerade Lösung $t = 2r, u = 2s$ von (171).

E. Sind t', u' und t'', u'' Lösungen, so auch das durch Multiplikation $2\varepsilon(t', u')\,\varepsilon(t'', u'') = t + u\sqrt{D}$ hervorgehende Paar t, u; denn es werden t und u ganz und

$$(182) \quad \varepsilon(t,u) \cdot \varepsilon(t,-u) = \varepsilon(t',u')\,\varepsilon(t'',u'')\,\varepsilon(t',-u')\,\varepsilon(t'',-u'') = 1.$$

Also wird $\varepsilon'\varepsilon'' = \varepsilon$ wieder Pellsche Einheit, ebenfalls ε^{-1} und $-\varepsilon^{\pm 1}$.

F. Die Potenzen der „Fundamentaleinheit" $E = \frac{1}{2}(T + U\sqrt{D})$ liefern bei $E > 1$ bereits unendlich viele Lösungen. (Für $D = -3$ und -4 entstehen hingegen bei $T \geqq 0$, $U > 0$ die zyklisch sich wiederholenden 6. und 4. Einheitswurzeln.)

G. Alle Pellschen Einheiten haben die Gestalt $\pm E^{\pm a}$. Es gäbe sonst ein ε mit $t, u > 0$, für das eine Ungleichung $E^n < \varepsilon < E^{n+1}$ gilt, und es wäre auch εE^{-n} eine Einheit $\varepsilon(t', u')$ zwischen 1 und E, also mit $0 < t' < T, 0 < u' < U$, entgegen der Definition von T, U.

Damit ist Satz 74 bewiesen. Wir fügen hinzu:

H. Die kleinste Lösung (181) liefert mit $t = 2r, u = s$ die kleinste für $t^2 - 4D \cdot u^2 = 4$, und für D selbst ist $2r = T_n, 2s = U_n$ und dabei $n = 1$ für $D \equiv 1$ (8), $n = 1$ oder 2 für $D \equiv 0$(4) und $n = 1$ oder 3 für $D \equiv 5$ (8), wie Rechnung ergibt. Vgl. hiermit (159) für $q = 2$!

I. Ist $t^2 - Du^2 = -4$ lösbar und $H = \frac{1}{2}(t + u\sqrt{D})$ die zugehörige „Nicht-Pellsche Einheit" mit der Norm -1, so wird $H^2 = E$ für kleinstes t, u. Aus $H^2 = TH + 1$, $H^n = tH^{n-1} + H^{n-2}$ folgen die Rekursionsformeln (176) wie (172) aus $E^2 = TE - 1$.

K. Die Überlegung von D. ist verallgemeinerungsfähig: Gehören zwei Darstellungen x, y und x', y' von $k = ax^2 + bxy + cy^2$ zur selben Schar, also

$$(183) \quad \begin{matrix} x' = \frac{1}{2}(t - bu)\,x - cuy; \quad y' = aux + \frac{1}{2}(t + bu)\,y, \\ xy' - yx' = (ax^2 + bxy + cy^2)\,u = ku. \end{matrix} \text{ so ist}$$

Ist umgekehrt $k \mid xy' - yx'$ $(y' : y \equiv x' : x \mod k)$, so gilt

$$(184)\quad 4k^2 = 4(ax^2+bxy+cy^2)(ax'^2+bx'y'+cy'^2)$$
$$= (2axx'+b(xy'+yx')+2cyy')^2 - D(xy'-yx')^2$$
$$= k^2\cdot(t^2-Du^2).$$

Setzt man die hier gewonnene Lösung der Pellschen Gleichung in (183) ein, so entstehen wirklich x' und y'. Man hat

Satz 75: Zwei Darstellungen einer Zahl k durch dieselbe Form gehören genau dann zur selben Schar (durch die Lösungen der Pellschen Gleichung ineinander übergehender Darstellungen), wenn sie mod k proportional sind

($x' \equiv jx,\ y' \equiv jy$ wie in (90) mit $j^2 \equiv 1 \bmod k$).

VI. Algorithmisches Rechnen.

§ 33. Allgemeines. Prüfung rationaler Rechnungen.

Algorithmen hatten wir in § 7, 25, 30 und 31: zur Bestimmung des größten gem. Teilers, des quadratischen Restcharakters und zur Reduktion der quadratischen Formen. Gemeinsam war den einzelnen Schritten dieser Algorithmen die Bestimmung einer Zahl durch Angabe eines Intervalls, in dem sie liegen soll, verbunden mit Kongruenzen, die sie erfüllen soll. Diese Rechenart, mit der wir auch die Ergebnisse des § 20 gewannen, wollen wir als *algorithmisch* bezeichnen. Sie liefert ein eindeutiges Ergebnis, wenn nur *ein* Rest nach einem die Intervallänge übertreffenden Modul in Frage kommt wie nachher bei den *Restproben*.

Meist ist es für zahlentheoretische Rechnungen vorteilhaft, mehrere Verfahren bereit zu haben, aus denen man das jeweils geeignetste wählt. Man vermeidet so auch Eintönigkeit im Rechnen und erwirbt sich ein weiteres heuristisches Bild über Zahleneigenschaften. Jedoch wird man die Auswahl auf wenige, etwa zwei bis drei Verfahren oder eine Mischung von zweien beschränken, da es oft nicht entschieden ist, welches das einfachste sei. Auch Verfahren, die nicht immer, meist dafür aber sehr schnell zum Ziel führen, wird man in der Zahlentheorie gern verwenden, um so mehr, als oft gleich nur wenige Lösungen in Frage kommen, die man allgemeine Rechnungen vermeidend schließlich einzeln prüfen kann.

Wir beginnen mit der Prüfung ganz-rationaler Rechnungen durch die bekannte Neuner- und Elferprobe sowie weitere Restproben. Haben wir etwa gerechnet $19 \cdot 379 = 7201$, so prüfen wir die Rechnung mod 9: Es ist $19 \equiv 1$;

$$379 \equiv 3 + 7 + 9 \equiv 1,$$

also $19 \cdot 379 \equiv 1$ und wirklich $7 + 2 + 0 + 1 \equiv 1 \bmod 9$. Eine Prüfung mod 11 ergibt

$$19 \equiv 9 - 1 = 8,\ 379 \equiv 9 - 7 + 3 = 5,$$

also $19 \cdot 379 \equiv 8 \cdot 5 \equiv -4$ und wirklich

$$7201 \equiv 1 + 2 - 7 = -4 \bmod 11.$$

Hätte man 7021 statt 7201 herausbekommen, so hätte man mod 9 noch nichts gemerkt; aber mod 11 stimmte die Rechnung nicht mehr. Man weiß also: wenn bei den Proben kein Rechenfehler gemacht wurde, ist 7021 bestimmt falsch gerechnet, 7201 hingegen *kann* richtig gerechnet sein und *ist* es sogar mod 99, auch mod $2 \cdot 99$, da eine ungerade Zahl herauskommen muß. Verbindet man jetzt aber diese Restproben mit einer Größenabschätzung, indem man das Ergebnis in ein Intervall von höchstens 198 aufeinanderfolgenden Zahlen einengt, so wird die Prüfung der Rechnung vollständig. Wir schätzen hier etwa ab:

$$19 \cdot 379 > 19 \cdot 375 = 19 \cdot \tfrac{3}{8} \cdot 1000 = 7\tfrac{1}{8} \cdot 1000;$$
$$19 \cdot 379 < 19 \cdot 380 = 7600\,(1 - \tfrac{1}{20}) < 7300.$$

Zwischen 7125 (auch 7100) und 7300 ist aber 7201 die einzige Zahl $\equiv 1 \bmod 2$, $1 \bmod 9$, $-4 \bmod 11$. Also ist 7201 *richtig, wenn alle Proben stimmen.* (Auf die Intervallänge legt man sich besser nicht gleich fest; dann schätzt man oben bequemer ab: $19 \cdot 380 < 20 \cdot 370 = 7400$; das Ergebnis liegt also zwischen 7100 und 7400, und es genügt nach der Neuner- und Elferprobe die weitere Feststellung, daß es von der Form $4n + 1$ sein muß, um eindeutig 7201 zu bekommen.) Anderes Beispiel:

$$Q = 256^2 + 37 \cdot 81^2 = 65536 + 999 \cdot 243 = 308293.$$

Abschätzung nach unten: $256^2 > 255^2 > 250 \cdot 260 = 65000$; $37 \cdot 81^2 > 37 \cdot 80^2 = 3700\,(27 \cdot 2 + 10) > 236000$. Nach oben

$256^2 < 260^2 = 67600; 37 \cdot 81^2 < 37 \cdot 6600 < (2000 + 37 \cdot 12) \cdot 100 < 245000$. Also $301000 < Q < 313000$.

Es genügt nun, den Rest von Q nach einem Modul $m < 12000$ zu bestimmen, etwa $m = 4 \cdot 9 \cdot 11 \cdot 41$. Wegen $100000 \equiv 1 \bmod 41$ (vgl. § 17 Ende) wird $308293 \equiv 8296 \equiv 96 \equiv 14 \bmod 41$, während einzeln $256 \equiv 10$, $256^2 \equiv 100 \equiv 18$; $37 \equiv -4$; $81^2 \equiv (-1)^2 = 1$; $Q \equiv 18 - 4 \cdot 1 \bmod 41$. Ebenso bestätigt man Kongruenz mod 4, 9, 11.

Selbst die *Ausführung* einer rationalen Rechnung gelingt oft schneller auf algorithmischem Wege; doch wird man hier schärfer abschätzen als bei den Rechenproben, um die Vereinigung vieler simultaner Kongruenzen zu vermeiden.

Beispiel: $P = 83 \cdot 167$. Aus $(x - z)(y + z) > x \cdot y$ für $x > y > z > 0$ folgt $13600 = 80 \cdot 170 < P < 90 \cdot 160 = 14400$. Letzte Ziffer: 1. Aus $P = 2 \cdot 5 \equiv 1 \bmod 9$, $\equiv -5 \cdot 2 \equiv 1 \bmod 11$, folgt dann $P = 13861$, da 1386 die einzige Zahl $\equiv 0 \bmod 9 \cdot 11$ zwischen 1360 und 1440.

$z = x^3 = 2713^3$. Man gewinnt aus $27^3 = 19683$ und $13^3 = 2197$ zuerst $z = 199 \ldots . 1097$, wobei die höchste der vier punktierten Stellen 6 oder 7 ist; die vorderen Stellen liefert die Abschätzung

$$2700^3 + 3 \cdot 2700^2 \cdot 13 < z < 2700^3 + 0{,}13(2800^3 - 2700^3),$$

zweite Glieder: $2187 \cdot 13 > 27700$; $13(28^3 - 27^3) < 29700$, zusammen: $(19683 + 277) \cdot 10^3 = 1996 \cdot 10^7 < z < 1998 \cdot 10^7$. Mod 10^4 ist $z \equiv 2197 + 3 \cdot 13^2 \cdot 2700 \equiv 1097$ bei

$$3 \cdot 13^2 \cdot 27 \equiv -11 \,(100).$$

Nun die mittleren Stellen: Wir setzen $z = 19960001097 + 10^4 y$; $0 \leqq y < 2000$. Mit $x \equiv 4\,(9)$ ist $x^3 \equiv 10\,(27)$ und mit

$$z \equiv 19 - 39 + 1 + 97 + 10y \bmod 27 \cdot 37$$

dann $y \equiv 4\,(27)$. Ebenso $y \equiv 17\,(37)$ bei $x \equiv 12\,(37)$. Vereinigt gibt das zuerst $y \equiv 17 - 37 \bmod 3 \cdot 37$ und bei

$$-20 \equiv 7,\ 3 \cdot 37 \equiv 3 \bmod 27$$

dann $y \equiv -20 - 111 \bmod 37 \cdot 27$. Also $y = 868$ oder 1867. Die Elferprobe entscheidet dann für $z = 19968681097$.

Die umgekehrte Aufgabe, die Kubikwurzel x zu bestimmen, wenn nur $z = 19 \ldots . . . 97$ als Kubus gegeben, ist leichter: die letzten zwei Stellen müssen 13 lauten; denn $x^3 \equiv 97\,(100)$ hat wegen $(97, 100) = (3, \varphi(100)) = 1$ nach (85) nur eine Lösung. Da z elfstellig ist, wird x vierstellig, und zwar $= 2713$, da $28^3 > 20000$ und

$26{,}13^3 < 19000$ ist, nämlich unter der Mitte von 26^3 und 27^3 liegt. Über die Einfachheit des Wurzelausziehens vgl. Ph. Männchen, Geheimnisse der Rechenkünstler, Math. Bibl. (Lietzmann), Bd. 13.

Zur 27er-Probe zeige man: Eine Zahl zwischen 000 und 999 ist genau dann durch 27 teilbar, wenn sie je eine Ziffer $p \equiv 1$, $q \equiv 2$ und $r \equiv 0 \bmod 3$ hat und bei der Ziffernfolge pqr, qrp, rpq die Quersumme 18, sonst aber die Quersumme 9.

§ 34. Lösung simultaner Auswahlkongruenzen.

Aufgabe (anschließend an § 15): Es sollen alle Zahlen der Form $8n + 3$ bestimmt werden, die quadratischer Rest für 3, 7, 11 und Nichtrest für 5 sind, ausführlich: die je eine der folgenden Kongruenzen erfüllen

$$(185) \quad x \equiv 3\,(8);\ x \equiv 1\,(3);\ x \equiv 2, 3\ (5);\ x \equiv 1, 2, 4\ (7);\ x \equiv 1, 3, 4, 5, 9\ (11).$$

Nach dem Reziprozitätsgesetz sind $-1; 2, 3, 5, 7, 11$ quadratische Nichtreste dieser x, und zu den Diskriminanten $D = -x$ gehören verhältnismäßig wenig reduzierte quadratische Formen und niedrige Klassenzahlen.

Lösung: $x \equiv 3\,(8), \equiv 1\,(3)$ gibt $x \equiv 19\,(24)$ und das mit $x \equiv 2, 3\,(5)$ vereinigt $x \equiv 43, 67\ (120)$. Diese Reste stellen wir zu ihrer Vereinigung mit $x \equiv 1, 2, 4\ (7)$ durch ihre Restklassen mod $120 \cdot 7 = 840$ dar:

$$(186) \quad x \equiv \begin{matrix} \underline{43} & \underline{163} & 283 & \underline{403} & 523 & 643 & 763 \\ \underline{67} & 187 & 307 & 427 & \underline{547} & \underline{667} & 787 \end{matrix} \bmod 840.$$

Die unterstrichenen Zahlen sind dabei die quadratischen Reste mod 7, die noch mit denen mod 11 zu vereinigen bleiben. Man erhält sie so: In (186) ist die Spaltendifferenz $120 \equiv 1\,(7)$, in der oberen Zeile $43 \equiv 1\,(7)$, also dort die erste, zweite, vierte Zahl zu unterstreichen; in der unteren Zeile ist aber $547 \equiv 1\,(7)$, die Unterstreichung gegen die obere Zeile somit um vier nach rechts „zyklisch" zu verschieben, d. h. man setzt die durch Addition von 120 sich wiederholenden Reste $67, 187, \ldots$ mod 840 rechts an und verschiebt dann. Die sechs Lösungen mod 840 stellen sich mod $840 \cdot 11 = 9240$ dar:

(187)

43	883	1723	2563	3403	4243	5083	5923	6763	7603	8443
67	907	1747	2587	3427	4267	5107	5947	6787	7627	8467
163	1003	1843	2683	3523	4363	5203	6043	6883	7723	8563
403	1243	2083	2923	3763	4603	5443	6283	7123	7963	8803
547	1387	2227	3067	3907	4747	5587	6427	7267	8107	8947
667	1507	2347	3187	4027	4867	5707	6547	7387	8227	9067

Die 30 unterstrichenen Reste mod 9240 sind jetzt die endgültigen Lösungen unserer Aufgabe. Man beginnt die Unterstreichung etwa in der mit den Resten $1, 5, 9, \ldots$ mod 11 beginnenden zweiten Zeile und sucht dann in jeder Zeile die Zahl auf, die $\equiv 1$ mod 11. Das „zyklische Verschieben" läßt sich nach der Methode von Kraitchik so erleichtern, daß man nach Festlegung eines Einheitsabstandes der Spaltenmitten in (187) einen Streifen

(188) $\underline{4}\ 8\ \underline{1}\ \underline{5}\ \underline{9}\ 2\ 6\ 10\ \underline{3}\ 7\ 0\ \underline{4}\ 8\ \underline{1}\ \underline{5}\ \underline{9}$

herstellt, dessen Zahlen im Einheitsabstand die Differenz $840 \equiv 4$ mod 11 haben, und auf dem alle Lösungsreste bis auf einen (hier 3) doppelt vorkommen. Diesen Streifen legt man jetzt in jeder Zeile von (187) so an, daß der Einzelsrest 3 unter der zu ihm kongruenten Zahl mod 11 liegt, und überträgt die Unterstreichungen auf die Zeile.

Soweit der Platz es zuläßt, tauscht man für dieses Streifenverfahren in (187) besser Zeilen und Spalten und bildet einen Längsstreifen (188). Läßt eine hinzukommende Auswahlkongruenz die Mehrzahl der Reste zu, so unterstreicht man besser die ausscheidenden.

Weitere Aufgabe: Alle $a < 100000$ aufzustellen, für die

(189) $$\left(\frac{-1}{a}\right) = \left(\frac{2}{a}\right) = \left(\frac{p}{a}\right) = -1 \quad \text{und} \quad \left(\frac{37}{a}\right) \neq 1.$$
(p Primzahl < 37)

Diese Eigenschaft besitzt z. B. die Zahl 163; § 30 gab (1, 1, 41) als einzige reduzierte Form der Diskriminante -163; wir suchen hier nun weitere im Verhältnis zu $\sqrt{D}$ niedrige Klassenzahlen.

Mit $a \equiv -1\,(4)$ formt sich die Aufgabe auf

$$(190)\quad a \equiv 3\,(8),\ \left(\frac{-a}{p}\right) = -1 \text{ für } p < 37,\ \left(\frac{-a}{37}\right) \neq 1$$

nach dem Reziprozitätsgesetz um. Man wird die Vereinigung der Kongruenzen etwa bis $p = 11$ wie oben vornehmen, dann die

$$(191)\quad x = r + sM < 100000,\ M = 9240,\ r \text{ aus } (187),$$

nehmen, unter denen die Lösungen von (189) zu suchen sind. Es sind für jedes $r < 7600$ die Werte $0 \leqq s \leqq 10$ zu untersuchen, für $r > 7600$ die $s \leqq 9$.

Nun bilde man für die Primzahlen $p = 13$ bis 37 je einen Längsstreifen der Länge $p + 10$ aus einer Folge von absolut kleinsten Resten der Differenz $M \bmod p$; hierbei $M \equiv -3 \bmod 13,\ -8 \bmod 17,\ 6 \bmod 19, \ldots, -10 \bmod 37$, und suche, (190) lösend, für jeden der 30 Werte $-r$ von unten her auf jedem der Streifen seinen Absolutrest auf, bringe diese Stellen der Streifen in eine Zeile und prüfe, ob in dieser oder einer der zehn darüberstehenden Zeilen lauter quadratische Nichtreste stehen oder bis $p = 31$ Nichtreste und der Rest 0 für $p = 37$. So liest man aus allen $-x = -r - sM$ recht schnell die $-a$ ab, die (190) erfüllen, und hat dann alle Lösungen a von (189). Wir erläutern dies hier für $r = 3763$:

p =	13	17	19	23	29	31	37	
.	.	.	.	.	.		.	
.	.	.	.	.	.		.	
.	.	.	.	.	.	.	.	
$-8M-r$ =	5	7	8	11	8	3	17	Lösung!
.	.	.	.	.	.	.	.	
$-M-r$ =	−3	2	−7	−8	−11	−14	−16	
$-r$ =	−6	−6	−1	9	7	−12	11	
	.		.	.		.	.	

Hat man so für jedes r die Streifen aufs neue aneinandergelegt, so erhält man als einzige Lösungen

$$163,\qquad 8M + 3763 = 77683 = 131 \cdot 593$$

$$\text{und}\quad 9M + 2347 = 85507 = 37 \cdot 2311.$$

Beiläufig haben die Diskriminanten — 77683 und — 85507 beide die Klassenzahl 22; die erste ist noch Nichtrest für 41 und 43, die zweite, durch 37 teilbare, noch für 41 bis 59; erst für diese ist $D : h^2 > 163$. — Die umgekehrte Aufgabe, — 1 und alle Primzahlen unter k, somit alle Zahlen zwischen $\pm k$ zu quadratischen Resten zu machen, ist bei Kraitchik Rc, S. 41/46 behandelt. Daß dort in den (186), (187) entsprechenden Schemen die teilerfremden Quadrate selbst auftreten, erleichtert die Unterstreichung wesentlich.

Da simultane Kongruenzen oft für alle Primzahlen unter einer Grenze aufgestellt werden, für die kleinsten Primzahlen teils in höherer Potenz (vgl. Primzahltafel § 35 und Kongruenzausscheidung § 36!), so lohnt es, etwa für

$$M = 2 \cdot 3 \cdot 5 \cdot 7 = 210,\ 2^3 \cdot 3 \cdot 5 \cdot 7 = 840,\ 2^5 \cdot 3^2 \cdot 5^2 = 7200,$$
$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 \quad \text{und} \quad 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 9240$$

Streifen mit der Restdifferenz M nach den niedrigsten zu M fremden p anzufertigen. Man wird die gegebene Simultankongruenz erst nach einem der M wie in (187) lösen, dabei im Auswahlfall M um so höher wählen, je weniger Kongruenzlösungen in Frage kommen und dann das Streifenverfahren anwenden. Bisweilen kommt man leichter auf ein M-Vielfaches; z. B. $x^2 \equiv 1 \bmod 630 \cdot 13 \cdot 19 \cdot 23$ liefert bald

$$x \equiv \pm 1,\ 41,\ 139,\ 181 \ (630).$$

Nun wird man aber die Streifen $p = 13, 19, 23$ von $M = 210$ nehmen und nur jede dritte Zeile ablesen. Auf diese Weise langt ein mäßiger Streifenvorrat für viele Kongruenzaufgaben.

§ 35. Primzahltafeln. Meißelsche Zählung.

Wir stellen als Aufgabe, unsere Primzahltafel aus § 9 über 300 hinaus fortzusetzen, etwa bis 100000. Wir denken daran, daß die Primzahlen zwischen n und $N \leqq n^2$ die dazwischenliegenden Lösungen der simultanen Auswahlkongruenz $x \not\equiv 0 \bmod p$ für alle $p \leqq n$ sind. Man kann also die Aufstellung einer Primzahltafel ganz als Kongruenzaufgabe in Teilabschnitten $n, N;\ N, N';\ \ldots$ mit steigender Kongruenzanzahl behandeln und wird darum mit Vorteil das Streifenverfahren aus § 34 verwenden können. Für dies wählen wir hier $M = 210$ und prüfen etwa mit zwanzig Streifen der

Differenz $M \bmod p$; $p = 11, 13, \ldots 89$ die nach Spalten des Schemas

(192)
$$\begin{array}{cccccccccccccc} 307 & 311 & 313 & 317 & 319 & 323 & 331 & 337 & 341 & \ldots & 457 & .. & 509 \\ 517 & 521 & 323 & 527 & 529 & 533 & 541 & 547 & 551 & \ldots & 667 & .. & 719 \\ 727 & 731 & 733 & 737 & 739 & 743 & 751 & 757 & \ldots\ldots & & 877 & .. & 929 \\ \ldots & & & & & & & & & & & & \\ 99847 & \ldots & & & & & & & & & 99997 & & \end{array}$$

geordneten 48 teilerfremden Restklassen mod M nach den zu 11 bis 89 primen Zahlen, die sich dadurch auszeichnen, daß auf den Streifen in ihrer Zeile kein Rest 0 ist. Da in (192) eine Spalte 475 Zahlen enthält, wird man zu ihrer Absuchung die Streifen öfters nachschieben müssen. Um dies für die kleinen p nicht zu oft zu tun, wählen wir ein Vielfaches $mp \geqq 37$ als Länge des p-Streifens, beginnend mit dem Rest von M, endigend mit 0.

Hat man so alle Zahlen unter 100000 ausgesiebt, die durch keine der Primzahlen bis 89 teilbar sind — einen p-Streifen brauchte man dabei immer erst ab p^2 anzusetzen — so ist die Primzahltafel bis 9400 fertig; oberhalb hat man aber noch zu streichen: $97 \cdot 97$ bis $97 \cdot 1021$, $101 \cdot 101$ bis $101 \cdot 983, \ldots$ bis $313 \cdot 317$; kurz: alle Produkte $pq < 100000$ zweier Primzahlen über 89; Produkte von mehr Primzahlen stehen nicht mehr da; sie müßten nämlich bei $47^3 > 100000$ wenigstens einen Faktor $\leqq 43$ haben. Die zu streichenden pq berechnet man am besten für jedes p nacheinander für die $q \geqq p$ durch Addition der häufig wiederkehrenden Differenzen.

Jetzt hat man die Primzahltafel bis 100000 fertig. Die vom gewöhnlichen Siebverfahren abweichende gemeinsame Aussiebung der Zahlen, deren kleinster Primteiler zwischen zwei Schranken (hier 10 und 90) liegt, verwendet in technischer Vervollkommnung neuerdings D. Lehmer zur Herstellung von Primzahltafeln über 10^7 hinaus.

Eine andere Möglichkeit wäre, die Aussiebung im Schema (192) graphisch vorzunehmen: man müßte dazu die Spalten des Schemas im natürlichen Abstandsverhältnis aufschreiben. Zur Ausscheidung z. B. der durch 11 teilbaren Zahlen verbinde man $319 = 11 \cdot 29$ in der ersten Zeile mit $517 = 11 \cdot 47$ in der zweiten, parallel dazu 341 (über die Stelle 539 der zweiten Zeile) mit 737 in der dritten Zeile, dieses nun in doppeltem und einfachem Abstand abwechselnd wieder-

holend. (Man trifft dabei als leere Stellen die Plätze der Zahlen mit kleinstem Primteiler 5 oder 7.) Dies Verfahren, ähnlich auf andere p angewandt, lohnt die Durchführung allenfalls bis $p = 61$; dann ist das halbe Schema schon gestrichen und der Übergang zur pq-Berechnung wie oben vorzuziehn.

Will man nun unsere Primzahltafel mit denselben Streifen etwa bis 10^3 fortsetzen, so hätte man schon sehr viele pq zu streichen, außerdem 97^3; $97^2 \cdot 101$, 103; $97 \cdot 101^2$. Doch ist diese Einteilung, bis $p = 89$ das Steifenverfahren anzuwenden, zur *Abzählung* der Primzahlen bis 10^6 noch sehr brauchbar. Macht man, um die Primzahlen bis z abzuzählen, den Schnitt bei $\sqrt[3]{z}$, so hat man die

Meißelsche Primzahlzählung. Es soll die Anzahl $\pi(z)$ der Primzahlen von 2 bis z bestimmt werden. Seien x und y die kleinsten Primzahlen mit $x^3 > z$ und $y^2 > z$. Ferner sei $V_m(n)$ die Anzahl der Zahlen von 1 bis n, die keinen Primteiler $p < m$ haben. Sodann gilt

$$\pi(z) = V_x(z) + \pi(x) - 2 - \sum_{x \leqq p < y} \left(\pi\left(\frac{z}{p}\right) - \pi(p) + 1 \right). \tag{193}$$

Denn $V_m(n)$ zählt für $n < m^2$ die Menge ab, die aus 1 und den Primzahlen von m bis n besteht; ihr sind die $\pi(m-1)$ Primzahlen unter m beizufügen und die Eins wegzunehmen, um die Anzahl $\pi(n)$ zu erhalten. Für $m^2 \leqq n < m^3$ muß man außerdem noch die Primprodukte pq mit $m \leqq p \leqq q \leqq \frac{n}{p}$ wegnehmen, um nur die Primzahlen bis n zu behalten, deren Anzahlen nach p geordnet für $n = z$ die Summanden rechts in (193) ergeben. Zu ihrer Feststellung braucht man bereits eine Primtafel bis $\frac{z}{x}$, also fast bis $z^{\frac{2}{3}}$. Das $V_x(z)$ berechnet man nach der Rekursionsformel

$$V_q(n) = V_p(n) - V_p\left(\frac{n}{p}\right); \quad p \text{ die Primzahl vor } q. \tag{194}$$

(Um V_q aus V_p zu erhalten, hat man die Vielfachen pv von p auszuscheiden, die, zugleich mit v, keinen Primteiler unter p haben; dabei $v \leqq \frac{n}{p}$.) Mit (194) bringt man ein V_q auf eine

V_{11}-Summe herab und verwendet

(195) $V_p(n) = \pi(n) - \pi(p) + 2$ für $n < p^2$, (s. o.),

(196) $V_q(kP + r) = k\,\varphi(P) + V_q(r)$ $\qquad P = \prod_{p<q} p$,

(197) $V_q(kP - r) = k\,\varphi(P) - V_q(r-1)$

(Es sind hier k reduzierte Restsysteme mod P zu nehmen, oben dazu nochmal die primen Reste von 1 bis r, unten aber die primen Reste von 0 oder -1 bis $-(r-1)$ einmal zu streichen.) Wir rechnen ein Beispiel durch:

$z = 30000$. Statt mit V_x, $x = 37$, fangen wir kürzehalber mit V_{29} an, haben dann nur außer den pq mit $29 \leqq p \leqq q$ noch 29^3, $29^2 \cdot 31$, $29 \cdot 31^2$ und 31^3 auszuschalten.

$$30000 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 - 30;\ \varphi(30030) = 5760.$$

$$V_{29}(30000) = V_{23}(30000) - V_{23}(1304), \qquad \text{nach (194)},$$
$$= V_{19}(30000) - V_{19}(1578) - V_{19}(1304) + V_{19}(68)$$
$$= V_{17}(30000) - V_{17}(1764) - V_{17}(1578) + 19 - V_{17}(1304) + 16 + 13$$

(für zweistellige Argumente nach (195) ausgerechnet)

$$= 5755 - V_{13}(1764) + 28 - V_{13}(1578) + 26 - V_{13}(1304) + 21 + 48$$
$$= 5878 - V_{11}(1764) + V_{11}(160) - V_{11}(1578) + V_{11}(143) - V_{11}(1304) + 27$$
$$= 5905 - V_{11}(84) - V_{11}(49) - V_{11}(108) - V_{11}(66) - V_{11}(44) - 48 \cdot 19$$

(Verwendung von (196/7) für $q = 11$ mit $P = 210$; $\varphi = 48$.)

$$= 4910.$$

Ausscheidende pq und pqr mit $p \geqq 29$. Anzahl: $1669 + 4$.

p	q	Anz.	p	q	A.	p	q	A.	p	q	A.
29	1034	165	61	491	77	101	297	37	139	215	14
31	967	153	67	447	68	103	291	35	149	201	12
37	810	129	71	422	63	107	280	32	151	198	10
41	731	117	73	410	60	109	275	30	157	191	7
43	697	112	79	379	54	113	265	27	163	184	5
47	638	101	83	361	50	127	236	21	167	179	3
53	566	88	89	337	45	131	229	19	173	173	1
59	508	80	97	309	39	137	218	15			

$$\pi(30000) = 4910 + \pi(29) - 2 - 1669 - 4 = 3245.$$

§ 36. Primprüfung und -zerlegung durch Quadratsummen.

Will man eine einzelne Zahl prüfen, ob sie Primzahl sei, wird man meist mit der Darstellung durch quadratische Formen am besten zu Rande kommen. Wir nehmen zuerst an, *die zu prüfende Zahl m sei von der Form* $4n + 1$. Wir wissen, daß es dann genau eine Darstellung $m = x^2 + y^2$ gibt (dabei $x \smile y$), wenn m Primzahl ist, sonst mehr oder keine. Wir prüfen so z. B. $m = 2713$. Ist $m = x^2 + y^2$, so $x, y \leqq 52$, und zwar hat man sofort die Lösung $y = 52$; $x = 3$. Es fragt sich, ob es noch eine gibt. Sei darin y wieder die gerade Zahl, so muß y durch 4 teilbar sein, damit x^2 zugleich mit $m \equiv 1 \bmod 8$. Wegen $m \equiv 4 \bmod 9$ muß x oder y durch 3 teilbar sein und die andere Zahl $\equiv \pm 2 \bmod 9$. Es kann danach noch $y = 12, 16, 20, 24, 36, 48$ sein, und wegen $m \equiv 3 \bmod 5$ bleibt davon nur $y = 12, 48$. Doch $2713 - 12^2$ und $2713 - 48^2$ sind keine Quadrate. Also ist $x = 3$; $y = 52$ die einzige Darstellung und m eine Primzahl.

Besonders, wenn m von der Form $20n + 1$ oder 9 ist, ist die Primprüfung durch $x^2 + y^2$ vorteilhaft und der durch $x^2 + 5y^2$ vorzuziehen. In diesem Falle muß nämlich x oder y durch 5 teilbar sein, weil die Summe zweier zu 5 fremden Quadrate $\equiv 0$ oder $\pm 2 \bmod 5$ ist. Sei also etwa $5 \mid y$, so untersuche man zuerst die Möglichkeit $10 \mid y$, also $x^2 \equiv m\,(100)$, was mod 100 vier Lösungen gibt, oder ein Paar $\pm a \bmod 50$, das man bald kennt. Für den andern Fall $y \equiv 5\,(10)$; $x^2 \equiv m - 25$ verwendet man

(198) $\quad y^2 \equiv 025, 225\ (1000)$ oder $625 \bmod 5000$,

vor allem $y \equiv 25\,(200)$, was schon nur das eine Paar $x \equiv \pm a \bmod 100$ zuläßt. Beispiele:

$m = 1501$. a) $x \equiv \pm 1\,(50)$; also $x = 1$, aber 1500 kein Quadrat. b) $x^2 \equiv 76\,(100)$; $x \equiv \pm 24\ (50)$, $= 24$ oder 26, aber $1501 - 576$, 676 nach (198) keine Quadrate. Also keine Darstellung $m = x^2 + y^2$ und m keine Primzahl.

$m = 6409$. a) $x \equiv \pm 3\,(50)$ liefert zwei Lösungen: $x = 3, 53$; $y = 80, 60$. Also m schon keine Primzahl. Näheres aus b) $x \equiv \pm 22\,(50)$, wo $x = 22 \bmod 200$ ausscheidet. Also $x \equiv \pm 28\,(100)$ mit zwei Lösungen $x = 28, 72$; $y = 75, 35$.

Nach Satz 46 ist dann 6409 ein Produkt von drei Primzahlen der Form $4n + 1$.

Bei größeren m wird man vor Untersuchung der Darstellungen $x^2 + y^2$ feststellen, ob etwa ein $p \leqq 13$ oder $p = 37 \mid m$, und hierzu $m \bmod 1001 = 7 \cdot 11 \cdot 13$ wie mod 999 reduzieren ($p = 2, 3, 5$ stets vorweggenommen). Auch wird man vor Ausrechnung der möglichen x mehr Kongruenzausscheidungen machen als oben bei $m = 2713$. Beispiel:

$m \equiv 129061$. $m \equiv 1\,(30)$; $\equiv 190\,(999)$; $\equiv 5\,(37)$; $\equiv -68\,(1001)$. Also ist m durch keins der genannten p teilbar (wegen $m = -68 + 1001 \cdot 129$ und $17 \mid 68$, $\nmid 129$ auch nicht durch 17, ebenso wegen der 190 oben nicht durch 19). Nach diesen Vorprüfungen suchen wir die Darstellungen $m = x^2 + y^2$ und nehmen $5 \mid y$. Aus $m \equiv 1\,(9)$ folgt $3 \mid xy$ und x oder $y \equiv \pm 1\,(9)$, aus $m \equiv 5\,(8)$, daß $y \equiv 2\,(4)$, also $y^2 \equiv 4\,(32)$ und bei $m \equiv 5\,(32)$ dann $x \equiv \pm 1\,(16)$, oder umgekehrt $x \equiv 2\,(4)$, $y \equiv \pm 1\,(16)$. Wie oben scheiden wir nach a) $y \equiv 0$ und b) $y \equiv 5\,(10)$.

a) $x \equiv \pm 19\,(50)$ und < 360 läßt bei $x \equiv \pm 1\,(16)$ zu: $x = 31, 81, 319$. Davon scheiden 31 und 319 mod 9 aus; doch $x = 81$ ergibt die Darstellung: $m = 81^2 + 350^2$.

b) $x \equiv \pm 6\,(100)$ wegen $x \equiv 2\,(4)$. Nach Ausscheidung mod 9 bleiben $x = 6, 206, 294, 306$ mit $m - x^2 \equiv 205, 625, 625, 425\,(1000)$, aber $\not\equiv 625\,(5000)$. Bliebe nur $x = 6$; aber $\frac{1}{25}(m - x^2) = 5161$ ist kein Quadrat.

Also ist $129061 = 81^2 + 350^2$ eine Primzahl.

$m \equiv 153949$. $m \equiv -11\,(30)$, $\equiv 103\,(999)$, $\equiv -205\,(1001)$. $m \equiv 5\,(8)$, $-3\,(32)$, $4\,(9)$, $-2\,(7)$, $4\,(11)$, $3\,(13)$.

a) $x \equiv \pm 7\,(50)$. Da $y^2 \equiv 4\,(32)$ wird, so $x^2 \equiv 25\,(32)$ und $x \equiv \pm 5\,(16)$. $m \equiv 4\,(9)$ gibt $x \equiv \pm 2\,(9)$ oder $3 \mid x$. Es bleiben mit $x < 400$ nur $x = 43$ und 357. Doch scheidet 357 wegen $m \equiv 5\,(7)$ aus; als Darstellung bleibt $m = 43^2 + 390^2$.

b) $x \equiv \pm 18\,(100)$. Nach Ausscheidung mod 9 bleiben $x = 18, 182, 218, 282, 318$, hiervon nach Ausscheidung mod 7 nur 218 und 282; doch ist $218^2 \equiv 282^2 \equiv 524\,(1000)$ und $m - 524 \equiv 425 \not\equiv y^2\,(1000)$. Also ist auch 153949 eine Primzahl.

Auch die Darstellung durch $x^2 + 37y^2$, die nach Satz 48 möglich ist, wenn $m = 4n + 1$ quadratischer Rest mod 37, entsprechend $x^2 + 13y^2$, wird man zur Verminderung des y besonders für $m \equiv 13, 17\ (20)$ heranziehn. Beispiel:

$$m = 308293 = x^2 + 37y^2 . \qquad y^2 < 8500;\ y < 93$$

$m - y^2 \equiv x^2 \bmod 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11$ erfordert

$y \equiv \pm 2\,(4)$ oder $1\,(8)$; $0\,(3)$ oder $4\,(9)$; $1\,(5)$ oder $8\,(25)$;
$\equiv \pm 1$ oder $3 \bmod 7$; $1, 3$ oder $4 \bmod 11$.

Die oberen Moduln lassen zu: $y = 6, 9, 31, 39, 49, 54, 66, 81, 86$; 33, 42, 58. Hiervon scheiden aber alle bis auf 81 mod 7 oder 11 aus. $m = 256^2 + 37 \cdot 81^2$ ist also Primzahl.

Endlich prüfen wir noch ein $m = 4n - 1$ durch $x^2 + 7y^2$. $m = 300007$. $m \equiv 1\,(7)$, also eindeutige Darstellung durch $x^2 + 7y^2$ für Primzahl entscheidend.

$m \equiv 7\,(32), 1\,(9), 7\,(25), 4\,(11)$ läßt zu:

$y \equiv \pm 1\,(8); 0\,(3), 7\,(9); 2\,(5), 1\,(25); 0, 2, 4, 5\,(11)$. Bleiben $y = 7, 33, 57, 97, 137, 183, 207$ mit $y \leqq 207$. Hiervon mod 37 nur 7 und 207 zulässig; einzige Lösung $x = 8$, $y = 207$.

Für Nichtreste m mod 7 bleiben noch $x^2 + 2y^2$ und $x^2 + 3y^2$ zur Probe. Alle versagen nur für $m \equiv 47, 143, 167\,(168)$.

Zieht man auch Darstellungen $m = x^2 + xy + cy^2$ mit $c = 3$, $5, 11, 17, 41$ heran, so versagen nur etwa zwei von tausend Fällen ganz.

Das Verfahren der Darstellung durch quadratische Formen ist auch zur Zerlegung von Zahlen mit mehreren Darstellungen brauchbar. Wir zeigen das unter Hinweis auf (89), aus dem folgende Rechnung hervorgeht, am Beispiel

$$m = 901 = 30^2 + 1^2 = 26^2 + 15^2.$$

Man bildet $(30 - 26) : (15 - 1) = 2 : 7$ und gewinnt den Faktor $2^2 + 7^2 = 53$; $901 = 53 \cdot 17$. Den Faktor 17 hätte man aus $(30 - 26) : (15 + 1) = 1 : 4$ gewonnen.

Ein andres, immer anwendbares und oft das beste Verfahren zur Zerlegung von ungeradem m ist das durch Darstellung $m = x^2 - y^2$. Hier gibt es stets die Darstellung $x - y = 1$, $x + y = m$ und nur sie, wenn m Primzahl. Zur Auffindung einer wirklichen Zerlegung $m = (x + y)(x - y)$

wird man m zuerst auf kleine Primteiler prüfen, um x in mäßigen Grenzen zu halten, sodann Kongruenzausscheidungen wie oben vorzunehmen. Beispiel:

$m = 29719$. Sei schon festgestellt, daß $p > 37$ für $p \mid m$. Dann $x - y \geqq 41$, $x + y < 725$ und $x < 400$; nämlich $x < x + y < m : 75 < 400$ für $x - y > 75$, sonst aber

$$(x + y) + (x - y) = 2x > 800.$$

Ferner $x \geqq 173$ und $4 \mid x \equiv \pm 1\,(9), \equiv \pm 12\,(25)$ oder $0\,(5)$. $x = 188, 388; 260, 280$. Mod 7 und 11 nur noch $x = 188$ mit $y = 75$. $m = 113 \cdot 263$.

§ 37. Index- und Restcharaktertafeln.

Eine Indextafel mod p^e, s. (82), kann man so aufstellen, daß man einen Primitivrest sucht, seine Potenzen mod p^e bildet und unter den ausgerechneten Rest jeweils den Exponenten schreibt. Primitivrest ist aber jeder Rest v, der für kein $q \mid \varphi(p^e)$ ein q-ter Potenzrest mod p^e ist, also für keinen Primteiler von $p - 1$ und bei $e \geqq 2$ auch nicht für $q = p$. Ist z. B. $p = 211$, $p - 1 = 2 \cdot 3 \cdot 5 \cdot 7$, so ist schon 2 kein quadratischer Rest, auch kein kubischer, da $211 \neq x^2 + 27y^2$, aber auch kein 5. oder 7. Potenzrest: es müßte sonst $(2^7)^6$ oder $(2^5)^6 \equiv 1\,(p)$ sein, also $32 \cdot 4$ oder 32 der Kongruenz

$$x^2 - x + 1 \equiv 0\,(p), \quad \text{also} \quad x^2 \equiv x - 1,$$

genügen (Exponent von 2^5 ist, s. o., mindestens 6); doch ist $32^2 \equiv -31$; $32^2 4^2 \equiv -496 \not\equiv 127\,(211)$. Also ist 2 Primitivrest mod p. Auch noch mod p^2, nämlich $2^{210} \not\equiv 1\,(211^2)$; man rechne nach, daß $2^{105} \equiv -1 + 51p$! Das kleinste p, für das $2^{p-1} \equiv 1\,(p^2)$, ist 1093; hier gilt bereits $2^{364} \equiv 1$ (s. u.).

Für $p = 439$ findet sich nicht sofort ein Primitivrest: Es ist $p - 1 = 2 \cdot 3 \cdot 73$; 2, 5, 7, 11, 13 quadratischer und 2, 3, 7 kubischer Rest ($439 = 243 + 14^2$, s. u.!); erst $3 \cdot 5$ ist beides nicht, aber auch kein 73. Rest; sonst hätte 15 den Exponenten 6, während $15^2 \not\equiv 14$. Also Primitivrest.

Um die Primitivreste aus den quadratischen Nichtresten leichter herauszufinden, wird man für die kleineren Primzahlen q eine Tafel der q-ten Potenzreste nach den $p \equiv 1\,(q)$, $p < N$, anlegen. Wir bringen hier auf S. 127 eine kubische

Kubische Restcharaktertafel.

	$2\ 3\ 5\ 7$	$11_{13}17_{19}$	$23_{29}31_{37}$	$2\ 3\ 5\ 7$	$11_{13}17_{19}$	$23_{29}31_{37}$	
61	1 0 1 1	0 1 2 2	0 2 2 0	1 1 2 0	1 1 2 2	0 2 1 2	463
67	1 0 0 2	2 1 1 1	1 2 2 1	1 1 0 0	1 2 2 0	1 0 1 0	487
73	1 0 2 0	2 1 0 1	2 1 1 2	0 0 1 1	2 0 1 1	2 2 0 0	499
79	1 1 2 2	2 1 0 2	2 2 2 1	1 0 1 2	0 2 0 2	2 2 2 1	523
97	1 1 1 1	2 1 2 0	2 1 1 1	1 2 1 0	1 1 0 2	2 0 1 1	541
103	1 0 2 2	2 0 2 1	0 1 0 0	1 0 2 1	1 1 1 2	2 0 0 1	547
109	0 1 1 1	2 1 0 0	0 1 2 2	1 2 1 0	2 2 1 2	0 1 0 1	571
127	0 1 0 1	2 1 2 0	1 2 1 2	1 0 1 2	0 2 1 0	2 0 2 0	577
139	1 2 2 2	1 1 2 1	0 1 2 2	0 1 1 1	1 0 2 1	1 1 0 2	601
151	1 0 1 1	1 2 1 0	1 0 1 1	1 2 2 0	1 2 2 1	1 2 1 0	607
157	0 1 1 0	1 2 1 1	0 0 2 2	1 0 2 1	2 1 1 0	0 1 0 0	613
163	1 2 0 1	2 0 0 2	0 2 0 0	1 0 1 2	1 0 0 2	1 0 0 2	619
181	1 2 0 0	2 2 1 0	2 0 0 2	1 2 0 1	1 1 2 2	1 2 2 2	631
193	1 0 1 2	0 0 1 1	0 0 1 2	0 0 0 1	2 1 2 1	2 1 2 2	643
199	1 1 0 1	0 1 0 1	1 1 2 2	1 0 2 0	2 0 1 0	2 2 0 1	661
211	1 1 0 1	0 0 1 1	0 2 1 1	1 1 2 0	2 1 1 1	0 2 2 0	673
223	0 1 2 0	2 0 0 1	1 2 1 2	0 1 0 2	2 2 2 0	2 2 0 1	691
229	0 1 2 2	0 0 0 2	1 1 2 1	1 1 1 1	1 0 1 1	1 2 1 1	709
241	1 2 0 1	1 2 0 1	0 1 1 1	0 0 1 1	0 2 1 2	0 1 1 1	727
271	1 0 2 1	1 0 2 0	0 0 0 1	0 1 0 1	0 2 1 0	1 0 2 1	733
277	0 1 2 2	2 0 2 0	2 1 1 0	0 1 0 1	1 0 1 2	1 1 2 0	739
283	0 1 2 2	2 2 2 0	1 0 1 2	1 2 2 0	2 2 1 2	2 2 1 1	751
307	0 0 1 2	1 1 0 0	2 2 2 1	1 0 1 1	2 2 2 2	2 0 2 2	757
313	1 2 0 0	1 1 1 0	0 2 1 1	1 1 0 0	2 2 0 2	1 1 2 2	769
331	1 1 2 0	2 1 1 2	1 1 1 2	1 0 1 1	1 1 1 2	2 2 0 1	787
337	1 2 0 0	0 1 0 1	1 2 2 1	0 1 2 0	1 1 1 0	2 0 1 0	811
349	1 2 2 1	0 1 0 2	1 2 0 0	1 1 0 1	0 2 2 0	2 0 2 1	823
367	1 0 0 0	1 1 1 2	2 0 1 2	1 1 2 0	0 1 2 1	2 0 0 2	829
373	1 1 1 0	2 0 0 0	0 2 0 2	1 0 0 0	2 0 2 1	1 1 1 0	853
379	1 2 0 2	1 1 1 1	0 0 1 0	1 2 2 1	0 0 2 2	1 1 1 2	859
397	0 1 2 1	1 1 0 1	1 1 0 1	1 2 1 1	0 2 0 2	2 0 1 1	877
409	1 2 0 2	0 0 1 0	1 2 0 1	1 1 1 0	2 1 0 2	2 1 0 0	883
421	1 2 2 0	1 0 1 0	1 0 2 0	1 1 2 2	0 2 2 0	0 1 2 2	907
433	0 1 1 2	1 1 1 1	2 1 1 0	0 0 1 2	2 0 0 2	2 0 1 1	919
439	0 0 1 0	2 2 1 1	2 2 1 1	1 2 1 2	2 2 1 2	0 2 1 2	937
457	0 1 0 2	0 1 0 2	1 2 2 0	1 0 2 2	0 2 0 1	0 0 2 2	967
				1 0 1 2	1 2 0 2	2 0 1 0	991
				0 0 0 1	1 1 2 2	2 2 0 0	997
				1 0 1 2	1 0 1 0	0 1 2 2	1009

Resttafel in der Form, daß wir für $60 < p < 1020$ den kubischen Restcharakter der Primzahlen a bis 37 vermerken durch Angabe des Exponenten $e = 0, 1, 2$ in der Kongruenz

(199) $a^n \equiv r^e \bmod p = 3n + 1$; r Rest der Ordnung 3.

Wir legen r dadurch fest, daß wir für den kleinsten kubischen Nichtrest $e = 1$ setzen. Ein Produkt der a ist dann kubischer Rest, wenn ihre e-Summe $\equiv 0\,(3)$. Die Ablesung ist hiernach für jeden Rest x nach einem p der Tafel so möglich: enthält x etwa Primteiler über 37, so führt mit 37 $x > p$ die Division $p = xy \pm z$ zu $x \equiv \pm \frac{z}{y}$ mit einem $y \leqq 37$ und $z \leqq \frac{1}{2} x$. Hat z noch einen großen Primteiler, so verfahre man mit dem wieder wie mit x. So erhält man bald einen Quotienten von Faktoren bekannten Restcharakters. Beispiel: 199 ist kubischer Rest mod 691; es ist $691 = 199 \cdot 4 - 105$ (besser als $199 \cdot 3 + 94$), $199 \equiv 3 \cdot 5 \cdot 7 : 4 \bmod 691$ und $e\,(199) \equiv 1 + 0 + 2 - 0 \bmod 3$.

Für die $p < 61$ geben wir alle kubischen Reste außer ± 1 an:

(200)

mod	13	19	31	37	43
$\pm$	5	7,8	2,4,8,15	6,8,10,11,14	2,4,8,11,16,21

Für $p \geqq 61$ verwende man dann die Tafel S. 127, deren Berechnung wir an zwei Beispielen erläutern. Zuerst sucht man den kleinsten kubischen Nichtrest, der $\leqq 7$ für $p < 5113$. Wir wissen: 2 ist kubischer Rest für die $p = x^2 + 27y^2$, und merken uns: 3 ist für diese p nur bei $3 \mid y$ kubischer Rest (allgemein für ein $p = x^2 + xy + 61y^2$), 5 nur bei $5 \mid xy$, 7 nur bei $7 \mid xy$ (11 schon nicht nur bei $11 \mid xy$), also 2, 3, 5 und 7 nur für ein $p = x^2 + 243z^2$ mit $35 \mid xz$. Nun sucht man p (auch $2p$) als Summe oder Differenz zweier Zahlen mit kleinen Primteilern und kubischen Faktoren darzustellen und erhält dann die Restcharaktere so:

$p = 211$. $p + x^2 + 27y^2$; $e(2) = 1$. $3^5 = p + 2^5$; $e(3) = 1$. $p + 5 = 6^3$; $e(5) = 0$. $p - 1 = 7 \cdot 30$; $e(7) = 1$. $p - 11 = 8 \cdot 5^2$; $e(11) = 0$. $p + 13 = 7 \cdot 2^5$; $e(13) = 0$. Jetzt $p = 17y + z$; ...(s. o.).

$p = 727$. $p = 22^2 + 243$; $e(2) = e(3) = e(11) = 0$. (Auch $p + 2 = 3^6$; $p - 1 = 6 \cdot 11^2$.) Kleinster Nichtrest 5; $e(5) = 1$.

$p-7=5\cdot 12^2$; $e(7)=1$. $p+1=13\cdot 7\cdot 8$; $e(13)=2$.
$p-13=17\cdot 42$; $e(17)=1$. $p-5=2\cdot 19^2$; $e(19)=2$.
$p+23=6\cdot 5^3$; $e(23)=0$. Jetzt das Divisionsverfahren.

Die so errechneten Werte kann man bereits als die mod 3 genommenen Indizes einer Indextafel auffassen. Trägt man in der kubischen Tafel für die $p\equiv 1(3^i)$, $\not\equiv 1(3^{i+1})$ gleich den 3^i-ten Restcharakter ein und bildet ebensolche 5^i-te, 7^i-te, ... Potenzresttafeln, so geht eine Indextafel mod p für $p-1=\Pi q^i$ aus den Werten der q^i-ten Potenzresttafeln als Simultankongruenz hervor. Beispiel:

$y=\text{ind } 79 \bmod 211$. $\left(\frac{79}{211}\right)=\left(\frac{-211}{79}\right)=\left(\frac{2}{79}\right)\left(\frac{13}{79}\right)=1$. $y\equiv 0(2)$

$79\equiv 2\cdot 13:3$ kubischer Rest. $y\equiv 0(3)$

5. Rest-	a	2	3	5	7	11	13
charakter	e_5	1	3	2	4	2	4
7. „	e_7	1	1	6	6	1	4

Erste Feststellung:
$-2^{10}\equiv 31\equiv 2\cdot 11^2$ $y\equiv 2(5)$
$3^7\equiv 77\equiv 2^5 3^2$ $y\equiv 4(7)$
$y\equiv 0(6)$; $\equiv -3(35)$: $y=102$.

Dabei wurde wirklich mit der Basis 2 gerechnet, weil in allen Potenzresttafeln $e(2)=1$ war. In diesen wurde aus $e(2)=1$ nach „erster Feststellung“ $e_5(11)=2$ und $e_7(3)=1$ gewonnen.

Will man in die Tafel nur die Indizes der kleinen Primzahlen aufnehmen, so ist das hier gewonnene Verfahren kürzer als das der Basispotenzierung. Man rechnet sogar $2^{102}\equiv 79$ (211) schneller über $\text{ind } 3=43$; $2^{102}\equiv 3^2\cdot 2^{16}$.

Man kann die Indextafel mod p für die kleinen Primzahlen, sobald man eine passende Basis v hat, auch ohne getrennte Potenzrestrechnung unmittelbar gewinnen, indem man Darstellungen $mp=A-B$ mit kleinen Primfaktoren sucht (jetzt ohne Multiplikation mit q-ten Potenzen, die für große $q\mid p-1$ ohnedies selten werden). Beispiel:

$p=439=2k+1$. $v=15$. $\begin{array}{cccccccc}\text{ind} & -1 & 2 & 3 & 5 & 7 & 11\\ = & k & x & y & 1-y & z & w\end{array}$

$p-7=2^4 3^3$. $p+2=3^2 7^2$.
$k+z\equiv 4x+3y$; $x\equiv 2y+2(4x+3y)$.
$p+11=15^2\,2$. $p+1=2^3 5\cdot 11$.
$w\equiv 2+x$; $4x+3-y\equiv 0(438)$.

Hieraus y in der zweiten Kongruenz eingesetzt gibt $39x \equiv -24\,(438)$ oder, da $6 \mid x$ bekannt, $13x \equiv -8\,(73)$. $x \equiv 5\,(73)$; $x = 78$.

Ähnlich verwertet E. Gottschalk (Math. Ann. 115, S. 157/8) Lösungsbedingungen der Fermat-Gleichung: Soll $x^p + y^p = z^p$ mit $xyz \smile p$ lösbar sein, so muß nach Morishima u. a. $r^{p-1} \equiv 1\,(p^2)$ für $r < 37$ gelten. Das geht aber nicht, wenn sich eine Zerlegung $mp = A \pm B$ mit $m < p$ findet, in der A und B nur Primfaktoren $\leqq 31$ haben; denn das gäbe $A^{p-1} \equiv (\pm B)^{p-1} \equiv 1\,(p^2)$ entgegen $(A - mp)^{p-1} \equiv A + Am^{p-2}p$. Für $p < 3600$ ist $p = 99q +$ oder $- r$ $(r < 99)$ eine solche Zerlegung, also die Fermatgleichung mit $xyz \smile p$ unlösbar. Wir betrachten eingehender

$$p = 1093 \quad = 2^2 3^5 + 11^2 = 3^2 11^2 + 4;\ 3^7 = 2p + 1.$$

Hiernach ist schon $3^{p-1} \not\equiv 1\,(p^2)$, auch 33^{p-1}, wenn $2^{p-1} \equiv 1\,(p^2)$. Dies prüfen wir: Oben erschien 2 als kubischer Rest und 3 mod p als Rest der Ordnung 7; bei $p - 1 = 3 \cdot 7 \cdot 52$ rechnen wir dann

$$2^{10} = p - 69;\ 2^{14} = 16p - 1104 = 15p - 11.\ 2^{52} = 2^{14 \cdot 3 + 10}.$$

$$2^{42} \equiv -11^3 + 3 \cdot 11^2 15p = -1331 + (p - 4)\,5p \equiv -238 - 21p$$

$$2^{52} \equiv 7\,(34 + 3p)\,(69 - p) \equiv 238 \cdot 69 + 7 \cdot 173p \qquad \mod p^2.$$
$$\equiv (3^5 - 5)\,3 \cdot 23 + 118p \equiv \tfrac{1}{3}\,((2p + 1)\,23 - p + 58) + 118p$$
$$= 27 + 133p.$$

$$2^{364} \equiv (27 + 133p)^7 \equiv (1 + 2p)^3 + 7 \cdot 133 \cdot 3^{18} p$$
$$\equiv 1 + 6p - 6 \cdot 3^3 \cdot 3^4 p \equiv 1\,(p^2).$$

Eine Indextafel mod p^2 liefern im wesentlichen schon die Indizes der Reste $1 - p, 2 - p, \ldots - 1; 1, 2, \ldots p - 1$. Man schreibe sie in zwei Zeilen auf und entnimmt dann

$$(201)\quad \operatorname{ind}(r + kp) = \operatorname{ind} r + k\,(\operatorname{ind} r - \operatorname{ind}(r - p)),\ k \bmod p,$$

aus den Indizes der r-ten Spalte. Ist nämlich $v^{p-1} = 1 + zp$, so mit (78) $rv^{(p-1)l} \equiv r + rlzp\,(p^2)$ und bei $k \equiv lrz\,(p)$

$$\operatorname{ind}(r + kp) = \operatorname{ind} r + (p - 1)\,l;\quad l \equiv k : rz\,(p).$$

Da $\operatorname{ind}(-r) = \operatorname{ind} r \pm \frac{1}{2}(p - 1)$, reicht eine Tafelhälfte:

mod 11^2 Reste:	-10	-9	-8	-7	-6	Indizes:	20	11	58	62	34
	1	2	3	4	5		0	1	88	2	74

Berechnung durch Potenzrestverfahren (die Zerlegung nach Charakteren ist hier wegen $3^5 \equiv 1\,(11^2)$ ratsam!) oder Bildung der Potenzen $\pm 2^c$, $c = 0, \ldots 9$, dabei z. B. die letzte Spalte

aus $4 = \text{ind}(5 + 11)$ und $64 = \text{ind}(5 - 33) = \text{ind}(-512)$ bei $9 = \text{ind}\,512$. — Will man nun ind 91 ablesen, zerlegt man

$$91 = 3 + 8 \cdot 11;\ \text{ind}\,91 \equiv 88 + 8 \cdot 30 \equiv 108\,(110).$$

Ebenso gewinnt man eine Indextafel mod p^e mit Zeilenabstand p^{e-1}.

§ 38. Auflösung der reinen Kongruenz.

Reine quadratische und kubische Kongruenzen löst man oft am einfachsten mit dem Differenzverfahren des § 37:

$z^3 \equiv 2 \mod p = 1093$. Zur Lösung nimmt man etwa $p + 2^5 = 3^2 5^3$; $p - 11^2 = 2^2 3^5$; $p - 5^3 = 2^3 11^2$. Daraus

$$4 : 9 \equiv \left(\frac{5}{2}\right)^3;\quad 4 \cdot 9 \equiv -\frac{11^2}{3^3} = \left(\frac{5}{6}\right)^3;\quad \text{also } 16 \equiv \left(\frac{25}{12}\right)^3.$$

Lösungen: $z \equiv \frac{25}{24} \cdot r^{0,1,2}$. $r \equiv \frac{x}{y}\,(p)$ aus $x^2 + xy + y^2 = p$.

$x^4 \equiv 17\,(257)$. Diese Aufgabe zerlege man in $y^2 \equiv 17$; $x^2 \equiv y$ und bilde

$$15^2 \equiv -32;\ 16^2 \equiv -1;\ 17^2 \equiv 32;\ 22^2 \equiv -30;\ 23^2 \equiv 15.$$

$$17 \equiv -240 \equiv -15 \cdot 16 \equiv (23 \cdot 16 \cdot 4)^2 \equiv 70^2.$$

$$x^2 \equiv \pm 70;\ -5 \cdot 14 \equiv 18 \cdot 14^2 \equiv \left(\frac{17}{4} \cdot 3 \cdot 14\right)^2 \equiv 50^2.$$

$$x \equiv \pm 50,\ \pm 29.$$

Höhere unzerlegbare Wurzelausziehungen wird man mit Indexrechnung machen. Schon, um eine Aufgabe $z^7 \equiv 6\,(463)$ nach obiger Art zu rechnen, wird man aus den brauchbaren Zerlegungen $p = A \pm B\,(A = 448, 450, 455, 462, 468, 484)$ schneller die Indizes von 2 bis 13 erhalten und aus ihnen dann $\text{ind}\,z = \frac{1}{7}\,\text{ind}\,6 + 66k$ zusammensetzen. $z \equiv -72 \cdot (-\frac{3}{2})^k$.

Zur Lösung der quadratischen Kongruenz mod p wird man jedoch vorzugsweise von Satz 48 Gebrauch machen, z. B.:

$z^2 \equiv 37\,(65537)$. Man zerlege hier $37 = (-1)(-37)$. Da -1 und -37 quadratische Reste sind, stellt sich das $p = x^2 + y^2 = v^2 + 37w^2$. $x = 256, y = 1$; $v = 122, w = 37$. Kongruenzlösung: $z \equiv 256 \cdot \frac{1}{37}\frac{2}{7}\frac{2}{} \equiv 13243$.

Versagt dieses und das Differenzverfahren, so liefert die

Darstellung $x^2 - Dy^2 = pt$, vgl. (202), ein zur Lösung von $z^2 \equiv D(p)$ allgemein geeignetes Verfahren. Beispiel:

$z^2 \equiv 257\ (65537)$. Für $ef > p$ (hier $p = 2^{16} + 1$) gibt es nach Satz 28 ein $x < e$ und ein $y < f$ mit $x : y \equiv z\,(p)$. Es wird $p \mid x^2 - 257y^2$ und für $e = 1025$ und $f = 64$

$$x^2,\ 257y^2 < 2^{20};\quad x^2 - 257y^2 = pt \quad \text{mit} \quad |t| < 16.$$

Jede Lösung x, y, t mit $x \smile y$ gibt eine Kongruenzlösung z. Wir ermitteln nun die Paare t, y, die ein x^2 liefern, durch Kongruenzausscheidung: Es muß t quadratischer Rest für 257 sein, außerdem ungerade oder durch 8 teilbar. Also

$t = -1,$	$+1,$	$-11,$	$+11,$	$-13,$	$+13,$	$-8,$	$+8.$
$y > 15$	$y < 64$	$y > 52$	$y < 56$	$y > 56$	$y < 28$	$y > 43$	$y < 48$
$\equiv \pm 1\,(8)$	$0\,(4)$	$2\,(4)$	$5\,(16)$	$9\,(16)$	$2\,(4)$	$1\,(2)$	$1\,(2)$
$2\,(5), 4\,(25)$	$1\,(5), 3\,(25)$		$1\,(5), 7\,(25)$	$0, 1\,(5)$	$0, 2\,(5)$	$0, 1\,(5)$	$0, 2\,(5)$
$0\,(3), 4\,(9)$	$1\,(3)$	$1\,(3)$	$0\,(3), 2\,(9)$		$1\,(3)$	$1\,(3)$	$0\,(3), 4\,(9)$

Unter den möglichen Werten t stehen oben: eine Schranke und Kongruenzbedingungen für zugehörige y, gewonnen aus

$$257y^2 = x^2 - pt$$

mit $x \leqq 1024$ und $F = 257y^2 + pt \equiv x^2\,(2^5 \cdot 5^2 \cdot 3^2)$.

(Ausrechnung wie in § 36 bei $m = 129061$ und 153949; $y \smile t$!)
Weiter:

$$-1\ {}^{23\ 33\ 57\ 63}_{\ 7\ \ 7\ 11} \qquad 1\ {}^{4\ 16\ 28\ 44\ 56}_{7\ 11^2\ 7\ 11\ 7} \qquad -11\ {}^{58\ 62}_{\ \ 13} \qquad 13\ {}^{2\ 10\ 22}_{7\ 11\ 37} \qquad t\ {}^{y}_{q}$$

$$-8\ {}^{49\ 55\ 59\ 61}_{13\ \ 1\ \ 7^2\ \ 7} \qquad 8\ {}^{3\ \ 5\ 13\ 15\ 23\ 27\ 33\ 45}_{7\ 13\ 11\ 13\ 11\ \ \ 13\ \ 7} \qquad 11\ {}^{21}_{\ 7} \qquad -13\ {}^{-}$$

Zu jedem t sind die hier zulässigen y zur weiteren Ausscheidung mod $q = 7, 11, 13, 37$; 7^2, 11^2 gesammelt und das kleinste der q, nach dem ein y ausscheidet, daruntergesetzt. Mod 7 wird so $F \equiv 5y^2 + 3t \equiv 4$; 2, 3, 0 für $y \equiv \pm 0$; 1, 2, 3 in $t = -8, -1, 13$. Dort scheidet also $y \equiv \pm 2$ aus und bleibt ± 3 bei $F \equiv 0\,(7)$ noch mod 49 offen.

Schließlich verbleiben die Paare $t = -1$, $y = 63$; $t = 8$, $y = 27$; $t = -11$, $y = 58$. Das letzte gibt $F = 379^2$. Also $x = 379$; $y = 58$. $\pm z \equiv \frac{3\,7\,9}{5\,8} = 6\frac{1}{2} + \frac{1}{29} \equiv 759\frac{5}{6} \equiv -10163$.

Allgemein ist so $z^2 \equiv D(p)$ durch eine Darstellung

$$(202)\quad x^2 - Dy^2 = pt \text{ mit } x \leqq \sqrt{p} \cdot \sqrt[4]{|D|},\ y \leqq \sqrt{p} : \sqrt[4]{|D|};$$
$$|t| < 2\sqrt{|D|}$$

lösbar, dabei $t > 0$ für $D < 0$ und $|t| < \sqrt{D}$ für $D > 0$. Große D kann man durch Brüche $-\frac{c}{a}$ ersetzen und dann $ax^2 + cy^2 = pt$ lösen; dadurch verkleinert man zwar selten das t, kann aber bei kleinzerfallenden a, c leichter mehr Kongruenzausscheidungen für t vornehmen.

Aus dem letzten Grunde rechnet man für kleines p mit $y = 1$, also ganzem $|z| < \frac{1}{2}p$ und $|t| < \frac{1}{4}p$.

Schließlich kann man auch die reine kubische Kongruenz durch eine Darstellung $ax^3 + cy^3 = pt$ lösen, kommt aber mit $|t|$ bis $2p$ statt bis $2\sqrt{p}$ wie in (202) hinauf, was nur bei starker Ausscheidungsmöglichkeit lohnt, etwa bei $91x^3 + 19y^3 = 919t$.

§ 39. Andere algebraische Kongruenzen.

Mit der Kongruenz $f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n \equiv 0 (p)$ wird man i. allg. auch so verfahren, daß man $z \equiv \frac{x}{y}$ darstellt und dann $a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n \equiv 0$ löst. Dabei läßt sich $f(z)$ für die in na_0 nicht aufgehenden p durch

$$h(z) \equiv \frac{1}{a_0} f\left(z - \frac{a_1}{na_0}\right) \equiv z^n + sz^{n-2} + \cdots + t$$

einfacher behandeln. Wir wählen ein kubisches Beispiel:

$f(z) = z^3 - 3z - 1 \equiv 0 (p)$ zu lösen $\begin{matrix} \text{A. für } p = 307, \\ \text{B. für alle } p \leqq 307. \end{matrix}$

In beiden Fällen reicht es,

$F(x, y) = x^3 - 3xy^2 - y^3$ für $0 \leqq x \leqq 21$ und $0 < |y| \leqq 13$ $(ef = 22 \cdot 14 = 308)$ zu betrachten, wobei wir das Vorzeichen von $z \equiv \frac{x}{y}$ dem y zuteilen, weil y nur in *einem* Glied von F nichtquadratisch ist. Im Fall A. reduziert man F für jedes x, y bald mod 307; bei B. aber rechnet man alle angegebenen $F(x, y)$ aus und zerlegt sie in Primfaktoren. Man wird hier erhalten: $f(z) \equiv 0 (p)$ hat je drei Wurzeln für die $p = 9n \pm 1$, eine dreifache Wurzel für $p = 3$, sonst keine Wurzel. (Erklärung s. u.).

Man untersuche ferner den kubischen Restcharakter der Wurzeln und findet sofort: entweder haben sie alle denselben oder alle ver-

schiedenen Restcharakter. Woraus folgt das hier? Wie verhalten sich die Fälle zum kubischen Charakter von 3 mod $p = 9n + 1$?

So groß der in der Verkleinerung der Summanden bestehende Vorteil der Ersetzung von $f(z) \equiv 0$ durch $F(x, y) \equiv 0$ gerade für Scharen von Kongruenzmoduln ist, so lohnen für einzelnes kleineres p, da man die Zahl der zu untersuchenden Fälle immerhin vermehrt, allenfalls Nenner $y = 2, 3$.

Manchmal läßt sich Probenverminderung erzielen: weiß man von $f(z) = z^3 + sz + t \equiv 0$ bereits, daß es keine oder drei Wurzeln mod p hat (das ist der Fall, wenn $D = -4s^3 - 27t^2$ quadratischer Rest für p), so braucht man nur die Reste $r = \pm 0, 1, \ldots, \left[\frac{p}{3}\right] - 1$ zu prüfen, ob sie $f(z) \equiv 0$ lösen; denn für den Fall dreier Wurzeln haben, wenn man ihre absolut kleinsten Reste nimmt, entweder alle Wurzeln gleiches Vorzeichen und eine Summe $r_1 + r_2 + r_3 = \pm p$, die ja mit dem z^2-Glied in f zugleich $\equiv 0(p)$, aber $< 2p$ ist; also ist eine der inkongruenten Wurzeln $\leqq \frac{p}{3} - 1$. Sonst aber ist etwa $r_3 = -r_1 - r_2$ und $|r_1| < \frac{p}{4}$; oder sogar $r_1 \equiv 0$. Man spalte dann $z - r_1$ von $f(z)$ ab und behält eine quadratische Kongruenz zu lösen.

Mod $p > 3$ besteht auch die Möglichkeit, eine Kongruenz 3. oder 4. Grades nach dem Schema der allgemeinen Gleichung 3. und 4. Grades mit Hilfe von Wurzelausziehungen aufzulösen, weil in den Nennern nur Potenzen von 2 und 3 auftreten. Eine Lösung im elementar zahlentheoretischen Sinne setzt jedoch voraus, daß bei Ausziehung einer n-ten Wurzel unter der Wurzel ein n-ter Potenzrest steht (Fall des § 38).

Andernfalls gäbe das eine Erweiterung des Restklassenkörpers mod p, deren Vergleich mit einer entsprechenden Erweiterung des Ringes der ganzen rationalen Zahlen einige Überlegung erfordert. Stellen wir den Vergleich aber für den Fall einer rationalen Kongruenzwurzel an, etwa $x^2 \equiv 2(7)$, so hat man ± 4 als rationale Kongruenzwurzel, im Ring V der $a + b\sqrt{2}$ mit ganzen a, b aber außerdem $\pm \sqrt{2}$, ohne daß dort $\sqrt{2} \equiv 4$ oder 3 mod 7 zu setzen ist, also vier Lösungen in V, vereinigt aus den je zwei Lösungen

$$\pm 4 \mod (7, 4 - \sqrt{2}) \text{ und } (7, 4 + \sqrt{2}),$$

vgl. § 27 Ende. Die Vielfachsummen von 7 und $4 - \sqrt{2}$ sind da-

bei die Vielfachen von $3 + \sqrt{2}$. Dies liegt anders in $R(\sqrt{30})$, wo die vier Lösungen $\pm 4, \sqrt{30}$ von $x^2 \equiv 2\,(7)$ sich auch aus denen mod $\mathfrak{p}, \mathfrak{p}' = (7, 4 \pm \sqrt{30})$ vereinigen, doch $\mathfrak{p}$ und $\mathfrak{p}'$ nicht aus den Vielfachen einer Zahl bestehen. Ebenso nicht die Moduln $\mathfrak{q}, \mathfrak{q}' = (13, 2 \pm \sqrt{30})$. Eine Kongruenz mod 91 ist in $R(\sqrt{30})$ die Vereinigung je einer Kongruenz mod $\mathfrak{p}, \mathfrak{p}', \mathfrak{q}, \mathfrak{q}'$. Jede paarweise Vereinigung dieser Kongruenzen liefert eine Kongruenz, deren Modul aus den Vielfachen einer der in $R(\sqrt{30})$ *unzerlegbaren* Zahlen 7, 13; $11 \pm \sqrt{30}$; $19 \pm 3\sqrt{30}$, *dreier Paare* mit dem *Produkt* 91, besteht.

Bei der Kongruenz $z^3 - z - 1 \equiv 0$ bestätigt sich nun wenigstens für die $p = 9n + 1$ die Existenz dreier Wurzeln daraus, daß die *Gleichungs*wurzeln die Summen einander reziproker neunter Einheitswurzeln sind und $x^9 - 1 \mod p = 9n + 1$ voll zerfällt.

Sach- und Namenverzeichnis.

Mathematische und verwandte Literatur
in Auswahl
WALTER DE GRUYTER & CO. / BERLIN W 35

a) AUS DER SAMMLUNG GÖSCHEN

Geschichte der Mathematik. Von Prof. Dr. Heinrich Wieleitner. 2 Bände. I: Von den ältesten Zeiten bis zur Wende des 17. Jahrhunderts. 136 Seiten. Neudruck 1939. II: Von 1700 bis zur Mitte des 19. Jahrhunderts. 154 Seiten. Neudruck 1939. (Samml. Göschen Nr. 226, 875) Geb. je RM. 1.62

Fünfstellige Logarithmen. Mit mehreren graphischen Rechentafeln und häufig vorkommenden Zahlwerten. Von Professor A. Adler. Zweite Aufl. 117 S. u. 1 Taf. 1929. (Samml. Göschen Bd. 423) Geb. RM. 1.62

Der Band enthält die gemeinen Logarithmen der ganzen Zahlen bis 1000, die der goniometrischen Funktionen, die wirklichen Werte dieser Funktionen und die Reihe von mathematischen, physikalischen und astronomischen Hilfstafeln, wie sie fünfstelligen Logarithmentafeln gewöhnlich beigegeben sind.

Vierstellige Tafeln und Gegentafeln für logarithmisches und trigonometrisches Rechnen in zwei Farben zusammengestellt. Von Professor Dr. Hermann Schubert. Neue Ausgabe von Dr. Robert Haußner, o. ö. Professor an der Universität Jena. 175 Seiten. Neue Auflage. 1938. (Samml. Göschen Bd. 81) . . . . . Geb. RM. 1.62

Mathematische Formelsammlung. Von Professor O. Th. Bürklen †. Vollständig umgearbeitete Neuausgabe von Dr. F. Ringleb. Mit 37 Figuren. Dritte, verbesserte Auflage. 272 Seiten. 1936. (Sammlung Göschen Bd. 51) . . . . . Geb. RM. 1.62

Formelsammlung zur praktischen Mathematik. Von Dr. Günther Schulz. Mit 10 Abbild. 147 S. 1937. (Sammlung Göschen Bd. 1110.) Geb. RM. 1.62

Mengenlehre. Von Professor Dr. E. Kamke. Mit 6 Figuren. 160 Seiten. 1928. (Samml. Göschen Bd. 999) . . . . . Geb. RM. 1.62

Arithmetik. Von Studienrat Prof. Paul B. Fischer. Mit 19 Abbildungen 152 Seiten. 1938. (Sammlung Göschen Bd. 47) . . . . Geh. RM. 1.62

Dieses Bändchen ist als einführendes Werk gedacht, es beschäftigt sich infolgedessen nur mit der niederen Arithmetik; einige weiterführende Dinge werden wenigstens gestreift. Sechs Abschnitte, Zählen und Zahlen (I), Bereich der natürlichen (II), ganzen (III), rationalen (IV), reellen (V), komplexen (VI) Zahlen, und ein Anhang über einfache arithmetische und geometrische Reihen, Zinseszins- und Rentenrechnung, Kombinatorik und den binomischen Lehrsatz stellen den äußeren Rahmen dar.

Elementare Algebra vom höheren Standpunkt. Von Dr. Wolfgang Krull, o. Professor an der Universität Bonn. Mit 6 Zeichnungen. 1939. (Sammlung Göschen Bd. 930.) . . . . . Geb. RM. 1.62

Höhere Algebra. Von Dr. Helmut Hasse, o. ö. Professor der Mathematik an der Universität Göttingen.

I: Lineare Gleichungen. Zweite, verbesserte Auflage. 152 Seiten. 1933. (Samml. Göschen Bd. 931) . . . . . Geb. RM. 1.62

II: Gleichungen höheren Grades. Zweite, verbesserte Auflage. Mit 5 Fig. 158 Seiten. 1937. (Samml. Göschen Bd. 932) Geb. RM. 1.62

Aufgabensammlung zur höheren Algebra. Von Dr. Helmut Hasse, o. ö. Professor der Mathematik an der Universität Göttingen. 160 Seiten. 1934. (Sammlung Göschen Bd. 1082) . . . . . Geb. RM 1.62

Einführung in die Zahlentheorie. Von Dr. Arnold Scholz, Dozent der Mathematik an der Universität Kiel. 136 Seiten. 1939. (Sammlung Göschen Band 1131) . . . . . Geb. RM. 1.62

Gruppentheorie. Von Dr. Ludwig Baumgartner in München. Mit 8 Figuren. 120 Seiten. 1921. (Samml. Göschen Bd. 837) . . . . . Geb. RM. 1.62

Determinanten. Von Studienrat Professor Paul B. Fischer. Dritte, verbesserte Auflage. Durchgesehener Neudruck. 136 Seiten. 1932. (Samml. Göschen Bd. 402) . . . . . Geb. RM. 1.62

Differentialrechnung. Von Prof. Dr. A. Witting, Oberstudienrat i. R. in Dresden. Zweite, verbesserte Auflage. Mit 94 Figuren und 189 Beispielen. 191 Seiten. 1936. (Samml. Göschen Bd. 87) . . Geb. RM. 1.62

Integralrechnung. Von Prof. Dr. A. Witting, Oberstudienrat i. R. in Dresden. Mit 63 Figuren und 190 Beispielen. 176 Seiten. 1933. (Samml. Göschen Bd. 88) . . . . . Geb. RM. 1.62

Repetitorium und Aufgabensammlung zur Differentialrechnung. Von Professor Dr. A. Witting. Mit 58 Figuren und 405 Beispielen und Aufgaben. 136 Seiten. 1935. (Samml. Göschen Bd. 146) . Geb. RM. 1.62

Repetitorium und Aufgabensammlung zur Integralrechnung. Von Prof. Dr. A. Witting. Mit 32 Figuren und 305 Beispielen. 118 Seiten. 1934. (Samml. Göschen Bd. 147) . . . . . Geb. RM. 1.62

Elementare Reihenlehre. Von Dr. Hans Falckenberg, Professor an der Universität Gießen. Mit 4 Figuren im Text. 136 Seiten. 1926. (Samml. Göschen Bd. 943) . . . . . Geb. RM. 1.62

Komplexe Reihen nebst Aufgaben über reelle und komplexe Reihen. Von Dr. Hans Falckenberg, Professor an der Universität Gießen. Mit 3 Figuren im Text. 140 Seiten. 1931. (Samml. Göschen Bd. 1027) . Geb. RM. 1.62

Gewöhnliche Differentialgleichungen. Von Prof. Dr. G. Hoheisel. Dritte, neubearbeitete Auflage. 126 Seiten. 1938. (Samml. Göschen Bd. 920) Geb. RM. 1.62

Partielle Differentialgleichungen. Von Prof. Dr. G. Hoheisel. 159 Seiten. 1928. (Samml. Göschen Bd. 1003) . . . . . Geb. RM. 1.62

Aufgabensammlung zu den gewöhnlichen und partiellen Differentialgleichungen. Von Professor Dr. G. Hoheisel. 148 Seiten. 1933. (Sammlung Göschen Bd. 1059) . . . . . Geb. RM. 1.62

Integralgleichungen. Von Prof. Dr. G. Hoheisel. 136 Seiten. 1936. (Samml. Göschen Bd. 1099) . . . . . Geb. RM. 1.62

Variationsrechnung I. Von Dr. Lothar Koschmieder, o. Professor an der Deutschen Technischen Hochschule in Brünn. Mit 21 Fig. 128 Seiten. 1933. (Samml. Göschen Bd. 1074) . . . . . Geb. RM. 1.62

Elemente der Funktionentheorie. Von Dr. Konrad Knopp, o. Prof. an der Universität Tübingen. Mit 23 Fig. 144 Seiten. 1937. (Samml. Göschen Bd. 1109.) . . . . . Geb. RM. 1.62

Funktionentheorie. Von Dr. Konrad Knopp, o. Professor an der Universität Tübingen.

Erster Teil: Grundlagen der allgemeinen Theorie der analytischen Funktionen. Mit 8 Figuren. Fünfte, verbesserte Auflage. 136 Seiten. 1937. (Samml. Göschen Bd. 668) . . . . . Geb. RM. 1.62

Zweiter Teil: Anwendungen und Weiterführung der allgemeinen Theorie. Mit 7 Figuren. Vierte, verbesserte Auflage. 138 Seiten. 1931. (Samml. Göschen Bd. 703) . . . . . Geb. RM. 1.62

Aufgabensammlung zur Funktionentheorie. Von Dr. Konrad Knopp, o. Professor an der Universität Tübingen.

Erster Teil: Aufgaben zur elementaren Funktionentheorie. Zweite, verbesserte Auflage. 136 Seiten. 1931. (Samml. Göschen Bd. 877) Geb. RM. 1.62

Zweiter Teil: Aufgaben zur höheren Funktionentheorie. 143 Seiten. 1928. (Samml. Göschen Bd. 878) . . . . . Geb. RM. 1.62

Einführung in die konforme Abbildung. Von Dr. Ludwig Bieberbach, o. ö. Professor an der Universität Berlin. Dritte Auflage. Mit 42 Zeichnungen. 136 Seiten. 1937. (Samml. Göschen Bd. 768). Geb. RM. 1.62

Ebene und sphärische Trigonometrie. Von Professor Dr. Gerhard Hessenberg. Mit 59 Figuren. Vierte Auflage. 171 Seiten. 1934. (Samml. Göschen Bd. 99) . . . . . Geb. RM. 1.62

Analytische Geometrie der Ebene. Von Dr. R. Haußner, o. ö. Professor an der Universität Jena. Zweite, verb. Auflage. Mit 60 Figuren. 164 Seiten. 1934. (Samml. Göschen Bd. 65) . . . . . Geb. RM. 1.62

Sammlung von Aufgaben und Beispielen zur analytischen Geometrie der Ebene mit den vollständigen Lösungen. Von Dr. R. Haußner, o. ö. Professor an der Universität Jena. Mit 22 Figuren im Text. 139 Seiten. 1933. (Samml. Göschen Bd. 256) . . . . . Geb. RM. 1.62

Analytische Geometrie des Raumes. Von Dr. Robert Haußner o. ö. Professor an der Universität Jena. Mit 36 Figuren im Text. 132 Seiten. 1935. (Samml. Göschen Bd. 89) . . . . . Geb. RM. 1.62

Koordinatensysteme. Von Professor Paul B. Fischer, Studienrat am Gymnasium zu Berlin-Steglitz. Mit 8 Figuren. Zweite, verbesserte Auflage. 128 Seiten. 1919. (Samml. Göschen Bd. 507) . . . Geb. RM. 1.62

Nichteuklidische Geometrie. Von Professor Dr. Richard Baldus. Mit 71 Figuren. 152 Seiten. 1927. (Samml. Göschen Bd. 970) . . Geb. RM. 1.62

Algebraische Kurven. Neue Bearbeitung von Prof. Dr. H. Wieleitner.

Erster Teil: Gestaltliche Verhältnisse. Mit 97 Figuren. Durchgesehener Neudruck. 146 Seiten. 1930. (Samml. Göschen Bd. 435) Geb. RM. 1.62

Zweiter Teil: Allgemeine Eigenschaften. Mit 35 Figuren. Neudruck. 123 Seiten. Neudruck 1939. (Samml. Göschen Bd. 436). Geb. RM. 1.62

Projektive Geometrie. Von Professor Dr. Karl Doehlemann. Neue einbändige Ausgabe von Dr. H. Timerding, Prof. an der Technischen Hochschule Braunschweig. Mit 37 Figuren. 131 Seiten. 1937. (Samml. Göschen Bd. 72) . . . . . Geb. RM. 1.62

Aufgabensammlung zur projektiven Geometrie. Von Dr. H. Timerding, Professor an der Technischen Hochschule Braunschweig. Mit 65 Figuren. 140 Seiten. 1933. (Sammlung Göschen Bd. 1060). . . . Geb. RM. 1.62

Differentialgeometrie I: Raumkurven und Anfänge der Flächentheorie. Von Dr. Rudolf Rothe, o. Professor an der Technischen Hochschule Berlin. Mit 32 Abbildungen. 132 Seiten. 1937. (Samml. Göschen Bd. 1113) . . . . . Geb. RM. 1.62

Vektoranalysis. Von Dr. Siegfried Valentiner, Professor für Physik an der Bergakademie Clausthal. Mit 16 Figuren. Fünfte, erneut durchges. Auflage. 136 Seiten. 1938. (Samml. Göschen Bd. 354) . Geb. RM. 1.62

Darstellende Geometrie. Von Dr. Robert Haußner, o. ö. Professor der Mathematik an der Universität Jena.

Erster Teil: Elemente; Ebenflächige Gebilde. Vierte, verbesserte Auflage. Mit 110 Figuren im Text. 207 Seiten. 1930. (Samml. Göschen Bd. 142) . . . . . Geb. RM. 1.62

Zweiter Teil: Perspektive ebener Gebilde; Kegelschnitte. Dritte, verbesserte und vermehrte Auflage. Mit 88 Figuren im Text. 168 Seiten. 1930. (Samml. Göschen Bd. 143) . . . . . Geb. RM 1.62

Dritter Teil: Zylinder, Kegel, Kugel, Rotations- und Schraubenflächen, Schattenkonstruktionen, Axonometrie. Von Dr. Robert Haußner, o. ö. Professor der Mathematik an der Universität Jena, und Dr. Wolfgang Haack, Dozent für Mathematik an der Technischen Hochschule Danzig-Langfuhr. Mit 65 Figuren im Text. 141 Seiten. 1931. (Sammlung Göschen Bd. 144) Geb. RM. 1.62

Vierter Teil: Freie und gebundene Perspektive, Photogrammetrie, kotierte Projektion. Von Dr. Robert Haußner, o. ö. Professor der Mathematik an der Universität Jena, und Dr. Wolfgang Haack, Dozent für Mathematik an der Techn. Hochschule Danzig-Langfuhr. Mit 76 Figuren im Text. 144 Seiten. 1933. (Samml. Göschen Bd. 1063). Geb. RM. 1.62

Wahrscheinlichkeitsrechnung. Von Professor Dr. Otto Knopf. I. 112 Seiten. 1923. II. Mit 10 Figuren. 112 Seiten. 1923. (Samml. Göschen Bd. 508 und 871) . . . . . Geb. je RM. 1.62

Ausgleichungsrechnung nach der Methode der kleinsten Quadrate. Von Professor Wilhelm Weitbrecht. Zweite, veränderte Auflage.

I. Teil: Ableitung der grundlegenden Sätze und Formeln. Mit 8 Figuren. Neudruck. 127 Seiten. 1938. (Samml. Göschen Bd. 302) Geb. RM. 1.62

II. Teil: Zahlenbeispiele. Mit 8 Figuren. Neudruck. 141 Seiten. 1920. (Samml. Göschen Bd. 641) . . . . . Geb. RM. 1.62

Versicherungsmathematik. Von Dr. Friedrich Böhm, Professor an der Universität München.

I. Elemente der Versicherungsrechnung. 2., vermehrte u. verbesserte Auflage. 144 Seiten. 1937. (Sammlung Göschen Bd. 180) Geb RM. 1.62

II. Lebensversicherungsmathematik. Einführung in die technischen Grundlagen der Sozialversicherung. 171 Seiten. 1926. (Samml. Göschen Bd. 917) . . . . . Geb. RM. 1.62

Der erste Band behandelt den Zins als erste, die Sterbetafel als zweite Rechnungsgrundlage, die Prämienreserve und die Versicherung verbundener Leben. Der zweite Band enthält außer einer eingehenden Behandlung der Lebensversicherungsmathematik eine Einführung in die technischen Grundlagen der Sozialversicherung.

Politische Arithmetik. (Zinseszinsen-, Renten- und Anleiherechnung.) Von Dr. Emil Foerster, Honorardozent an der Technischen Hochschule in Wien. Mit 7 Figuren. 155 Seiten. 1924. (Samml. Göschen Bd. 879) Geb. RM. 1.62

Graphische Darstellung in Wissenschaft und Technik. Von Professor Dr. M. Pirani. Zweite, verbesserte Auflage, besorgt durch Dr. J. Runge. Mit 71 Abbildungen. 149 Seit. 1931. (Samml. Göschen Bd. 728) Geb. RM. 1.62

Von der einfachen Darstellung von Größen mit unbekanntem Zusammenhang in Form von Kurven oder Skalen ausgehend, geht der Verfasser zur Darstellung von Größen bekannter Abhängigkeit (Funktionsskalen, insbesondere logarithmische projektive Teilung) über und bespricht dann die Aufstellung von Rechentafeln namentlich mit der Methode der fluchtrechten Punkte oder mit Hilfe mehrerer gekreuzter Linien.

Numerische Integration. Von Professor Dr. Fr. A. Willers. Mit 2 Figuren. 116 Seiten. 1923. (Samml. Göschen Bd. 864) . . . . Geb. RM. 1.62

Graphische Integration. Von Professor Dr. Fr. A. Willers. Mit 53 Figuren. 142 Seiten. 1920. (Samml. Göschen Bd. 801) . . . . Geb. RM. 1.62

Praktisches Zahlenrechnen. Von Professor Dr.-Ing. P. Werkmeister. Mit 60 Figuren. Zweite, verbesserte Auflage. 136 Seiten. 1929. (Samml. Göschen Bd. 405). . . . . Geb. RM. 1.62

Mathematische Instrumente. Von Professor Dr. Fr. A. Willers. Mit 68 Figuren. 144 Seiten. 1926. (Samml. Göschen Bd. 922) . . Geb. RM. 1.62

Geodäsie (Landesvermessung u. Erdmessung). Von Prof. Dr. Gustav Förster. Mit 33 Figuren. 122 Seiten. 1927. (Samml. Göschen Bd. 102) Geb. RM. 1.62

Vermessungskunde. Von Professor Dr.-Ing. P. Werkmeister.

I: Stückmessung und Nivellieren. Mit 145 Figuren. Sechste Auflage. 162 Seiten. 1938. (Samml. Göschen Bd. 468) . . . Geb. RM. 1.62

II: Messung von Horizontalwinkeln, Festlegung von Punkten im Koordinatensystem. Absteckungen. Mit 93 Figuren. Vierte Auflage. 147 Seiten. 1939. (Samml. Göschen Bd. 469) . . . Geb. RM. 1.62

III: Trigonometrische und barometrische Höhenmessung. Tachymetrie und Topographie. Mit 63 Figuren. Dritte Auflage. 144 Seiten. 1934. (Samml. Göschen Bd. 862) . . . . . Geb. RM. 1.62

Graphische Statik mit besonderer Berücksichtigung der Einflußlinien. Von Dipl.-Ing. Otto Henkel, Bauingenieur und Studienrat an der Baugewerkschule in Erfurt. 2 Teile. 1929. (Samml. Göschen Bd. 603 u. 695). Geb. RM. 1.62

Statik. I. Teil: Die Grundlagen der Statik starrer Körper. Von Professor Dr.-Ing. Ferd. Schleicher in Berlin. Mit 47 Abbildungen. 143 Seiten. 1930. (Samml. Göschen Bd. 178) . . . . . Geb. RM. 1.62

Dynamik. Von Prof. Dr. Wilhelm Müller. I: Dynamik des Einzelkörpers. Mit 70 Figuren. 160 Seiten. 1925. (Samml. Göschen Bd. 902) Geb. RM. 1.62
II: Dynamik von Körpersystemen. Mit 51 Figuren. 137 Seiten. 1925. (Samml. Göschen Bd. 903) . . . . . Geb. RM. 1.62

Hydraulik. Von Professor Dipl.-Ing. W. Hauber in Stuttgart. Zweite, verbesserte und vermehrte Auflage. Neudruck. Mit 45 Figuren. 156 Seiten. 1925. (Samml. Göschen Bd. 397) . . . . . Geb. RM. 1.62

Das Buch enthält eine Darstellung der Hydrostatik und bringt aus der Hydrodynamik: Ausfluß des Wassers aus Gefäßen; Überfall des Wassers über Wehre; Die Bewegung des Wassers in Flüssen und Kanälen; Die Bewegung des Wassers in Röhren mit konstantem Querschnitt; Stoß eines zylindrischen oder prismatischen Wasserstrahls auf eine Zylinderfläche.

Elastizitätslehre für Ingenieure. Von Professor Dr.-Ing. Max Enßlin an der Höheren Maschinenbauschule Eßlingen. 2 Bde. (Samml. Göschen Bd. 519 und 957) . . . . . Geb. je RM. 1.62

Einführung in die geometrische Optik. Von Dr. W. Hinrichs, Berlin-Wilmersdorf. Mit 56 Figuren. Zweite, verbesserte Auflage. 143 Seiten. 1924. (Samml. Göschen Bd. 532) . . . . . Geb. RM. 1.62

Technische Tabellen und Formeln. Von Reg.-Baurat a. D. Prof. Dr.-Ing. W. Müller. Mit 105 Figuren. Dritte, verbesserte und erweiterte Auflage. 151 Seiten. 1930. (Samml. Göschen Bd. 579) . . . . . Geb. RM. 1.62

b) WEITERE LITERATUR

Journal für die reine und angewandte Mathematik. Gegründet von A. L. Crelle 1826. Herausgegeben von Helmut Hasse. Band 1—140 Preise auf Anfrage, Band 141—144 je RM. 16.—, Band 145—147 je RM. 12.—, Band 148—151 je RM. 10.—, Band 152 RM. 12.—, Band 153 RM. 17.50, Band 154 RM. 30.—, Band 155 u. 156 je RM. 36.—, Band 157 u. 158 (Jubiläumsband I/II), Band 159—166 je RM. 36.—, Band 167 RM. 56.—, Band 168 RM. 36.—, Band 169 RM. 35.—, Band 170 RM. 35.—, Band 171—180 je RM. 30.—.

Das von A. L. Crelle gegründete „Journal für die reine und angewandte Mathematik" darf auf eine über hundertjährige ruhmvolle Vergangenheit zurückblicken. Seit seiner Gründung im Jahre 1826 wurde es der Sammelplatz für die Arbeiten der großen Männer, welche seit dieser Zeit der Mathematik einen neuen Aufschwung gaben.

Jahrbuch über die Fortschritte der Mathematik. Herausgegeben ab Band 51 von der Preußischen Akademie der Wissenschaften. Schriftleitung: Helmut Grunsky. Jeder der neueren Jahrgänge umfaßt 8—9 Hefte à 10 Druckbogen. Preis jedes Heftes RM. 18.—. Die Preise der früheren Jahrgänge werden auf Wunsch mitgeteilt.

Das „Jahrbuch über die Fortschritte der Mathematik" bringt eingehende Besprechungen sämtlicher periodischen und nichtperiodischen Neuerscheinungen auf dem Gebiete der Mathematik und ihrer wichtigsten Anwendungen. Auch die Geschichte und die Grundlagen der Mathematik finden sorgfältige Berücksichtigung.

Das Jahrbuch kann ab Band 51 (1925) nicht nur als Ganzes, sondern auch in einzelnen Sonderheften bezogen werden. Jedes Sonderheft umfaßt einen oder zwei der Hauptabschnitte des Jahrbuchs. Es erscheinen folgende Sonderhefte: I. Geschichte. Grundlagen der Mathematik. Abstrakte Mengenlehre. II. Arithmetik und Algebra. III. Analysis. IV. Geometrie. V. Angewandte Mathematik. — Preise auf Anfrage.

Geschichte der Mathematik. I. Teil: Von den ältesten Zeiten bis Cartesius. Von Professor Dr. S. Günther in München. Mit 56 Figuren. VIII, 428 Seiten. Neudruck 1927. (Samml. Schubert Bd. 18) . Geb. RM. 17.40

II. Teil: Von Cartesius bis zur Wende des 18. Jahrhunderts. Von Prof. Dr. Heinrich Wieleitner. 1. Hälfte: Arithmetik, Algebra, Analysis. Mit 6 Figuren. VIII, 251 Seiten. 1911. (Samml. Schubert, Bd. 63.) Geb. RM. 8.40. 2. Hälfte: Geometrie und Trigonometrie. Mit 13 Figuren. VI, 220 Seiten. 1921. (Samml. Schubert Bd. 64) . . . . Geb. RM. 3.50

Geschichte der Elementar-Mathematik in systematischer Darstellung. Von Professor Dr. Johannes Tropfke, Oberstudiendirektor i. R., Berlin. Lexikon-Oktav.

Band 1: Rechnen. VII, 222 Seiten. 3. Aufl., 1930. RM. 12.—, geb. RM. 13.20

Band 2: Allgemeine Arithmetik. IV, 266 Seiten. 3. Aufl., 1933. RM. 12.—, geb. RM. 13.20

Band 3: Proportionen, Gleichungen. IV, 239 Seiten. 3., verbesserte u. vermehrte Aufl., 1937 . . . . . RM. 10.—, geb. RM. 11.—

Band 4: Ebene Geometrie. IV, 240 Seiten. 2. Aufl., 1922. RM. 9.—, geb. RM. 10.—

Band 5: I. Ebene Trigonometrie. II. Sphärik und sphärische Trigonometrie. IV, 185 Seiten. 2. Aufl., 1923. RM. 7.50, geb. RM. 8.50

Band 6: Analysis, Analytische Geometrie. IV, 169 Seiten. 2. Aufl., 1924. RM. 7.—, geb. RM. 8.—

Band 7: Stereometrie. Verzeichnisse. V, 128 Seiten. 2. Aufl., 1924. RM. 6.50, geb. RM. 7.50

Mathematische Forschung in den letzten 20 Jahren. Rede, gehalten am 31. Januar 1921 vor der Mathematischen Gesellschaft Benares von deren Vorsitzendem Ganesh Prasad. Aus dem Englischen übersetzt von Dr. Friedrich Lange. Groß-Oktav. 37 Seiten. 1923 . . . . RM. 0.80
Dasselbe in englischer Sprache. 1923 . . . . . RM. 0.80

Neue Rechentafeln. Für Multiplikation und Division mit allen ein- bis vierstelligen Zahlen. Herausgegeben von Professor Dr. J. Peters, Observator am Astronomischen Recheninstitut. Folio-Format. VI, 500 Seiten. 1909 . . . . . Geb. RM 20.—
Diese Rechentafeln von Peters sind ebenfalls in französischer wie englischer Ausgabe zu haben . . . . . Geb. je RM. 20.—

Dr. A. L. Crelles Rechentafeln, welche alles Multiplizieren und Dividieren mit Zahlen unter Tausend ganz ersparen, bei größeren Zahlen aber die Rechnung erleichtern und sicherer machen. Neue Ausgabe. Besorgt von O. Seeliger. Mit Tafeln der Quadrat- und Kubikzahlen von 1—1000. VII, 501 Seiten. Folio. 1938. Geb. RM. 22.—
Diese Rechentafeln von Crelle liegen auch in englischer und französischer Ausgabe vor. Geb. je RM 22.—

Rechen-Resultate. Tabellen zum Ablesen der Resultate von Multiplikationen und Divisionen bis $100 \times 1000 = 100\,000$ in Bruchteilen und ganzen Zahlen sowie für Rechnen mit Zahlen jeder Größe, Radizieren (Wurzelsuchen) nach vereinfachtem Verfahren. Von F. Triebel, Technischem Oberinspektor der Reichsdruckerei i. R. Sechste Auflage, 21.—25. Tausend. Mit Seitenregistern. 290 Seiten. (Verlag von M. Krayn, Berlin). Geb. RM 18.—

Fünfstellige Logarithmentafeln der trigonometrischen Funktionen für jede Zeitsekunde des Quadranten. Herausgegeben von Prof. Dr. J. Peters, Observator am Astronomischen Recheninstitut. Lexikon-Oktav. IV, 82 Seiten. 1912 . . . . . Geb. RM. 7.—

Vollständige logarithmische und trigonometrische Tafeln. Von Professor Dr. E. F. August. Neunundvierzigste Auflage in der Bearbeitung von Professor Dr. F. August. Oktav. VII, 204 Seiten. 1931 Geb. RM. 2.—

Vierstellige Logarithmentafeln. Von Professor Dr. Max Zacharias und Dr. Paul Meth. Groß-Oktav. 43 Seiten. 1927 . . . . . Geb. RM. 1.50

Logarithmische Rechentafeln für Chemiker, Pharmazeuten, Mediziner und Physiker. Gegründet von Professor Dr. F. W. Küster †. Für den Gebrauch im Unterrichtslaboratorium und in der Praxis berechnet und mit Erläuterungen versehen. Nach dem gegenwärtigen Stande der Forschung bearbeitet von Dr. A. Thiel, o. ö. Professor der physikalischen Chemie, Direktor des Physik.-Chem. Instituts der Universität Marburg. Einundvierzigste bis fünfundvierzigste Auflage. Oktav. 216 Seiten. 1935 . . . . . Geb. RM. 6.80

Fünfstellige Tafeln der Kreis- und Hyperbelfunktionen sowie der Funktionen e^x und e^{-x} mit den natürlichen Zahlen als Argument. Von Dr.-Ing. Keiichi Hayashi, Professor an der Kaiserlichen Kyushu-Universität Fukuoka-Hakosaki, Japan. Oktav. IV, 182 Seiten. Neudruck 1938. RM. 9.—

Der bekannte japanische Verfasser hat aus der Notwendigkeit, die Werte beider Funktionsarten gleichzeitig zur Verfügung zu haben, Tafeln berechnet, in denen nicht nur die Hyperbelfunktionen, sondern auch die Kreisfunktionen mit verschieden großen Abstufungen, auf fünf Dezimalstellen angewendet sind. Die Anordnung dieser Tafeln ist äußerst praktisch, Druck und Papier sind ausgezeichnet, so daß die Benutzung sich bequem und einfach gestaltet. Für alle, die zahlenmäßige Rechnungen mit den genannten Funktionen häufiger auszuführen haben, ist der Gebrauch der Tafeln als praktisch und zeitsparend zu empfehlen.

Mathematische Mußestunden. Eine Sammlung von Geduldspielen, Kunststücken und Unterhaltungsaufgaben mathematischer Natur. Von Prof. Dr. Hermann Schubert. Fünfte Auflage, neu bearbeitet von Professor Dr. F. Fitting, München-Gladbach. Oktav. 260 Seiten. 1935. Geb. RM. 4.80

Dieses bekannte hier in der 5. Auflage erscheinende Buch wendet sich in erster Linie an den mathematischen Laien, den es in leichtfaßlicher und spannender Form in das Wesen der verbreiteten mathematischen Spiele einführen will. Doch sind auch einzelne Abschnitte aufgenommen, welche sich, oft durch kleineren Druck gekennzeichnet, hauptsächlich an den mathematisch interessierten Leser wenden und diesem Anregungen zu eigenen Untersuchungen auf dem Gebiete der Unterhaltungsmathematik geben wollen.

Lehrbuch der Mathematik für Studierende der Naturwissenschaften und der Technik. Eine Einführung in die Differential- und Integralrechnung und in die analytische Geometrie. Von Professor Dr. Georg Scheffers. Mit 438 Fig. Siebente Aufl. Lex.-Okt. VIII, 743 S. 1938 Geb. RM. 15.—

Dieses vor allem für Studierende der Naturwissenschaften und der Technik geschriebene Lehrbuch ist in erster Linie für den Selbstunterricht bestimmt und geht daher von dem denkbar geringsten Maß von Vorkenntnissen aus: der Leser braucht nur im Buchstabenrechnen, in der Auflösung von Gleichungen ersten Grades mit einer Unbekannten und in der niederen Geometrie bewandert zu sein.

Lehrbuch der höheren Mathematik für Universitäten und Technische Hochschulen, bearbeitet nach den Vorlesungen von Dr. Gerhard Kowalewski, o. Prof. an der Technischen Hochschule zu Dresden, o. Mitglied der Sächsischen Akademie der Wissenschaften zu Leipzig. 3 Bände. 1933. Jeder Band ist einzeln käuflich. . . . . Geb. je RM. 3.80

I. Vektorrechnung und analytische Geometrie.
II. Hauptpunkte der analytischen Geometrie des Raumes. — Grundbegriffe der Differential- und Integralrechnung.
III. Fortsetzung der Differential- und Integralrechnung. — Differentialgleichungen. Differentialgeometrie. Funktionen einer komplexen Veränderlichen. — Probleme der Variationsrechnung.

„. . . Klare und anschauliche Darstellung, mathematische Strenge, pädagogisches Geschick in der Verwertung der jeweils geeigneten Methoden (ich weise auf die durchgängige Verwendung der Vektorrechnung hin), Geschlossenheit in

dem Sinn, daß alle Hilfsmittel, die für die Darstellung nötig sind, in dem Werk selbst bereitgestellt werden, Allgemeinheit der leitenden Gesichtspunkte und Weite des Blicks sowie Veranschaulichung der vorgetragenen Theorien durch geeignete Anwendungen zeichnen es aus."

Unterrichtsblätter für Mathematik, Nr. 5, 1935.

Grundbegriffe und Hauptsätze der höheren Mathematik, insbesondere für Ingenieure und Naturforscher. Von Dr. Gerhard Kowalewski, o. Professor an der Technischen Hochschule zu Dresden. Mit 40 Figuren. Groß-Oktav. 156 Seiten. 1938 . . . . . Geb. RM. 5.—

Dieses Buch will den jungen Ingenieuren und Naturforschern behilflich sein, die Grundbegriffe und Hauptsätze der höheren Mathematik klar zu erfassen. Es stützt sich auf eine fast 40-jährige Lehrerfahrung des Verfassers an Universitäten und Technischen Hochschulen. Angesichts der starken Zurückdrängung der Mathematik in den Lehrplänen unserer höheren Schulen ist es an den Hochschulen mehr denn je notwendig, mit allen Mitteln vereinfachender Darstellungskunst dafür zu sorgen, daß wenigstens die Grundkenntnisse der höheren Mathematik fest angeeignet werden, ohne die ein gedeihliches Studium der Technik und Naturwissenschaft undenkbar ist. Hierbei will dieses Buch mithelfen. Inhalt: Vektorrechnung und Determinantentheorie. — Lehre von den Grenzwerten. — Differential- und Integralrechnung.

Einführung in die Axiomatik der Algebra. Von Dr. H. Beck, o. Professor an der Universität Bonn. X, 197 Seiten. 1926. (Göschens Lehrbücherei Bd. 6) . . . . . RM. 9.—, geb. RM. 10.50

Das vorliegende Buch enthält im wesentlichen den Stoff einer an der Bonner Universität gehaltenen Anfängervorlesung; es erschöpft sich nicht in axiomatischen Dingen, sondern bringt darüber hinaus eine Reihe anderer Gebiete, die der Studierende braucht.

Algebra I: Die Grundlagen. Von Dr. Oskar Perron, o. ö. Professor an der Universität München. Zweite, verbesserte Auflage. Mit 4 Figuren. VIII, 301 Seiten. 1932. (Göschens Lehrbücherei Bd. 8) Geb. RM. 11.50

Algebra II: Theorie der algebraischen Gleichungen. Von Dr. Oskar Perron, o. ö. Professor an der Universität München. Zweite, verbesserte Auflage. Mit 5 Figuren. VIII, 261 S. 1933. (Göschens Lehrbücherei Bd. 9) Geb. RM. 9.50

Band I enthält die Grundbegriffe, es folgt ein Kapitel über den polynomischen und den Taylorschen Satz und der für den Ingenieur wichtige Abschnitt über Determinanten. Anschließend folgen Kapitel über symmetrische Funktionen Teilbarkeit und über die Existenz von Wurzeln. Band II ist der Gleichungstheorie gewidmet.

Einführung in die Determinantentheorie einschließlich der Fredholmschen Determinanten. Von Dr. Gerhard Kowalewski, o. Professor an der Technischen Hochschule in Dresden. Zweite, verbesserte Auflage. Groß-Oktav. IV, 304 Seiten. 1925 . . . . . RM. 14.—, geb. RM. 15.50

Grundlehren der neueren Zahlentheorie. Von Professor Dr. Paul Bachmann. Dritte, neu durchgesehene Auflage. Herausgegeben von Dr. Robert Haußner, ord. Professor an der Universität Jena. Mit 10 Figuren. XVI, 252 Seiten. 1931. (Göschens Lehrbücherei Bd. 3) RM. 9.50, geb. RM. 10.50

Synthetische Zahlentheorie. Von Dr. Rudolf Fueter, o. Professor an der Universität Zürich. Zweite, verbesserte Auflage. VIII, 276 Seiten. 1925. (Göschens Lehrbücherei Bd. 4) . . . . . RM. 10.—, geb. RM. 12.—

Das Fermatproblem in seiner bisherigen Entwicklung. Von Professor Dr. Paul Bachmann. Oktav. VIII, 160 Seiten. 1919 . . . . RM. 2.50

In der vorliegenden Abhandlung gibt der Verfasser eine Übersicht von den Beweisverfahren und den Theorien, welche Euler, Legendre, Gauß, Dirichlet, Kummer und andere Forscher in ihren Studien über das allgemeine Fermatproblem angewandt und entwickelt haben.

Irrationalzahlen. Von Dr. Oskar Perron, o. ö. Professor an der Universität München. Zweite, durchges. Aufl. VIII, 199 Seiten. 1939. (Göschens Lehrbücherei Bd. 1) . . . . . Geb. RM. 9.80

Komplex-Symbolik, eine Einführung in die analytische Geometrie mehrdimensionaler Räume. Von Prof. Dr. Roland Weitzenböck. (Sammlung Schubert Band LVII.) Gr. 8° VI, 191 S. 1908. Geb. RM. 6.40

Reihenentwicklungen in der mathematischen Physik. Von Dr. Josef Lense, o. ö. Professor der Technischen Hochschule München. Mit 30 Abbildungen. 178 Seiten. 1933. . . . . Geb. RM. 9.50

Gewöhnliche Differentialgleichungen. Von Dr. J. Horn, em. o. Professor an der Technischen Hochschule Darmstadt. Dritte Auflage. Mit 4 Figuren. VIII, 195 Seiten. 1937. (Göschens Lehrbücherei Bd. 10). Geb. RM. 10.50

Partielle Differentialgleichungen. Von Dr. J. Horn, em. o. Professor an der Technischen Hochschule Darmstadt. Zweite, umgearbeitete Auflage. Mit 8 Figuren. VIII, 228 Seiten. 1929. (Göschens Lehrbücherei Bd. 14) RM. 11.—, geb. RM. 12.—

Grundzüge und Aufgaben der Differential- und Integralrechnung nebst den Resultaten. Von Dr. H. Dölp. Neu bearbeitet von Dr. Eugen Netto, 18. Auflage. Oktav. 214 Seiten. 1935. (Verlag von Alfred Töpelmann, Berlin W 35.) . . . . . RM. 1.95

Das Bändchen stellt eine elementare Aufgabensammlung zur Differential- und Integralrechnung mit eingefügten Erläuterungen dar. Der erste Abschnitt, Differentialrechnung für Funktionen einer und mehrerer Veränderlichen, bringt die Differentiation der elementaren Funktionen, einschließlich implizite Funktionen, die Ermittlung der Werte unbestimmter Formen, Maxima und Minima, Taylorsche Reihe. Der zweite Abschnitt, Integralrechnung, führt das Integral als unbestimmtes ein, entwickelt die Integrationsformeln im Bereiche der elementaren Funktionen und geht dann kurz auf das bestimmte Integral ein. Schließlich werden noch verhältnismäßig ausführlich geometrische Anwendungen der Infinitesimalrechnung gebracht: Tangentenbestimmung, singuläre Punkte, Krümmung; Quadratur, Rektifikation, Kubatur.

Integralgleichungen. Von Dr. Gerhard Kowalewski, o. Professor an der Technischen Hochschule Dresden. Mit 11 Figuren. Groß-Oktav. 302 Seiten. 1930. (Göschens Lehrbücherei Bd. 18) . . RM. 15.—, geb. RM. 16.50

Differential- und Integralrechnung. Unter besonderer Berücksichtigung neuerer Ergebnisse. Von Dr. Otto Haupt, Professor an der Universität Erlangen. Unter Mitarbeit von Dr. Georg Aumann, Professor an der Universität Frankfurt (Main). Groß-Oktav. 1938.

1. Band: Einführung in die reelle Analysis. Mit 2 Figuren. 196 Seiten. Geb. RM. 11.20
2. Band: Differentialrechnung. 168 Seiten . . . . . Geb. RM. 9.80
3. Band: Integralrechnung. 183 Seiten . . . . . Geb. RM. 10.60

(Göschens Lehrbücherei Band 24, 25, 26.)

Der erste Band bringt alles für das Verständnis der Differential- und Integralrechnung Erforderliche und damit zugleich eine Einführung in die wichtigsten Begriffsbildungen und Verfahren der reellen Analysis überhaupt. In Rücksicht auf den Anfänger, welcher noch keine weitgehenden Kenntnisse besitzt, werden die benötigten Hilfsmittel im Buche selbst entwickelt. Unbeschadet der Wahrung eines elementaren Standpunktes werden dabei auch

neuere, insbesondere für die Anwendungen wichtige Betrachtungsweisen herangezogen. Im zweiten Bande erscheint die Integralrechnung lediglich als Umkehrung der Differentialrechnung, während sie im dritten Bande ausgehend von der Lehre vom Flächeninhalt entwickelt wird. Im Rahmen eines elementaren Standpunktes werden dabei auch neuere wichtige Ergebnisse dargestellt, die in einführenden Lehrbüchern bis jetzt noch nicht behandelt worden sind. Für das Verständnis des einzelnen Bandes ist lediglich das erforderlich, und dies nur gelegentlich, was in den vorausgehenden Bänden schon entwickelt wurde.

Funktionentheoretische Vorlesungen. Von Heinrich Burkhardt. Neu herausgegeben von Dr. Georg Faber, o. Professor an der Technischen Hochschule in München.
I. Band 1. Heft. Dritte, umgearbeitete Auflage. Groß-Oktav. X, 182 Seiten. 1920 . . . . . RM. 6.—, geb. RM. 7.20
I. Band 2. Heft. Fünfte, umgearbeitete Auflage. Groß-Oktav. X, 286 Seiten. 1921 . . . . . RM. 9.—, geb. RM. 10.50
II. Band. Dritte, vollständig umgearbeitete Auflage. Groß-Oktav. VI, 444 Seiten. 1920 . . . . . RM. 14.—, geb. RM. 15.50

Elliptische Funktionen. Von Dr. R. König, o. Professor der Mathematik an der Universität Jena, und Dr. M. Krafft, a. o. Professor an der Universität Marburg i. H. Mit 4 Figuren. 263 Seiten. 1928. (Göschens Lehrbücherei Bd. 11) . . . . . RM. 13.—, geb. RM. 14.50

Elliptische Funktionen. Von Dr. Karl Boehm, Professor an der Technischen Hochschule Karlsruhe.
I. Teil: Theorie der elliptischen Funktionen aus analytischen Ausdrücken entwickelt. Mit 11 Figuren. Oktav. XII, 356 Seiten, Neudruck 1930. (Samml. Schubert Bd. 30) . . Geb. RM. 20.—
II. Teil: Theorie der elliptischen Integrale. Umkehrproblem. Mit 28 Figuren. Oktav. VII, 180 Seiten. 1910. (Samml. Schubert Bd. 61) Geb. RM. 7.80

Einführung in die Theorie der algebraischen Funktionen einer Veränderlichen. Von Heinrich W. E. Jung, o. ö. Professor an der Universität Halle-Wittenberg. Mit 35 Abbildungen im Text. Groß-Oktav. VI, 246 Seiten. 1923 . . . . . RM. 3.50, geb. RM. 4.—

Grundlagen der Geometrie. Von Professor Dr. Gerhard Hessenberg. Herausgegeben von Dr. W. Schwan. Mit 77 Figuren. 143 Seiten. 1930. (Göschens Lehrbücherei Bd. 17) . . . . . RM. 6.50, geb. RM. 7.80

Inhalt: I. Gleichheit, Ordnung und Stetigkeit. II. Die Messung durch Zahlen. (Streckenmessung, Winkelmessung, Flächenmessung.) III. Die projektive Geometrie in der Ebene. (Der Fundamentalsatz. Analyse des Fundamentalsatzes. Beweis des Fundamentalsatzes.) IV. Die projektive Geometrie im Raume. (Der Fundamentalsatz. Der Desarguessche Satz. Die Koordinatengeometrie.) V. Künstliche Geometrien.

Grundzüge der ebenen Geometrie. Von Professor Dr. F. Bohnert in Hamburg. Mit 220 Figuren. VIII, 223 Seiten. 1915. (Samml. Schubert Bd. 2) Geb. RM. 3.90

Ebene und sphärische Trigonometrie. Von Prof. Dr. F. Bohnert in Hamburg. Zweite Auflage. Dritter Neudruck. Mit 63 Figuren. VIII, 167 Seiten. 1919. (Samml. Schubert Bd. 3) . . . . . Geb. RM. 4.40

Einführung in die analytische Geometrie. Von Professor Dr. Gerhard Kowalewski. Mit 112 Figuren. Dritte, unveränderte Auflage. Lexikon-Oktav. VIII, 360 Seiten. 1929 . . . . . Geb. RM. 11.20

Das aus Vorlesungen entstandene Buch ist namentlich zum Gebrauch für Studierende bestimmt.

Elementargeometrie der Ebene und des Raumes. Von Professor Dr. Max Zacharias, Studienrat in Berlin. Mit 196 Figuren im Text. 252 Seiten. 1929. (Göschens Lehrbücherei Bd. 16) . . . RM. 13.—, geb. RM. 14.50

Die Elementargeometrie wird nicht vom Standpunkte des Schulunterrichts, sondern von dem der Wissenschaft aus behandelt. Ausgangspunkt ist das (etwas modifizierte) Hilbertsche Axiomensystem. In der Darstellung treten zwei Momente in den Vordergrund: die geschichtliche Entwicklung und die prinzipielle Begründung der einzelnen Gebiete.

Analytische Geometrie auf der Kugel. Von Dr. Richard Heger, Professor an der Technischen Hochschule in Dresden. Mit 4 Figuren. (Sammlung Schubert Bd. LIV.) Gr.-Oktav. VII, 152 S. 1908 . . . Geb. RM. 5.20

Punkt- und Vektor-Rechnung. Von Dr. Alfred Lotze, Professor für Mathematik an der Technischen Hochschule Stuttgart. Mit 7 Figuren. 192 Seiten. 1929. (Göschens Lehrbücherei Bd. 13) . . . RM. 12.—, geb. RM. 13.—

Kreis und Kugel. Von Dr. Wilhelm Blaschke, o. Prof. a. d. Univ. Hamburg. Mit 27 Fig. im Text. Groß-Oktav. X, 169 S. 1916. RM. 4.40, geb. RM. 5.50

Liniengeometrie mit Anwendungen. Von Professor Dr. Konrad Zindler in Innsbruck. I. Teil. Mit 87 Figuren. Neudruck. VIII, 380 Seiten. 1928. (Samml. Schubert Bd. 34) . . . . . Geb. RM. 18.—
II. Teil. Mit 24 Figuren. VII, 252 Seiten. 1906. (Samml. Schubert Bd. 51) Geb. RM. 9.50

Projektive Liniengeometrie. Von Dr. Robert Sauer, Prof. an der Technischen Hochschule Aachen. Mit 36 Abbild. Groß-Oktav. 194 Seiten. 1937. (Göschens Lehrbücherei Bd. 23) . . . . . Geb. RM. 9.—

Geometrische Transformationen. Von Dr. Karl Doehlemann, weil. Professor an der Technischen Hochschule München. Zweite Auflage, herausgegeben von Dr. Wilhelm Olbrich, Professor an der Hochschule für Bodenkultur in Wien. Mit 89 Figuren im Text und 4 Abbildungen. 254 Seiten. 1930. (Göschens Lehrbücherei Bd. 15) RM. 13.—, geb. RM. 14.50

Vorlesungen über allgemeine natürliche Geometrie und Liesche Transformationsgruppen. Von Dr. Gerhard Kowalewski, o. ö. Professor der reinen Mathematik an der Technischen Hochschule zu Dresden. Mit 16 Figuren. Groß-Oktav. 280 Seiten. 1931. (Göschens Lehrbücherei Bd. 19) RM. 15.50 geb. RM. 17.—

Affine Differentialgeometrie. Von Dr. Erich Salkowski, o. Professor an der Technischen Hochschule Berlin. Groß-Oktav. Mit 23 Figuren. 200 Seiten. 1934. (Göschens Lehrbücherei Bd. 22) . . . . . Geb. RM. 10.—

Die vorliegende Darstellung ist aus Vorlesungen hervorgegangen, die der Verfasser an den Technischen Hochschulen Hannover und Berlin gehalten hat. Das Ziel dieses neuen Bandes von Göschens Lehrbücherei ist, den Anfänger, dem nur die Grundtatsachen der Vektorrechnung und der Differentialgeometrie geläufig sein müssen, mit den Begriffsbildungen der Tensorrechnung vertraut zu machen, die für das Verständnis der neueren differential-geometrischen und mathematisch-physikalischen Forschung unentbehrlich sind. Dabei wurde darauf Bedacht genommen, von den einfachsten, allgemein bekannten Tatsachen ausgehend und in dauernder Verbindung mit der geometrischen Anschauung den Formelapparat der Ricci-Rechnung allmählich so zu entwickeln, daß er dem Lernenden nicht als ein analytisches Kunststück entgegentritt, sondern sich als ein naturgemäßes Hilfsmittel der geometrischen Forschung aufbaut. Aus diesem Grunde wurde die Untersuchung auf die einfachsten Gegenstände beschränkt und grundsätzlich nur zweidimensionale analytische Gebilde betrachtet.

Anwendung der Differential- und Integralrechnung auf Geometrie. Von Professor Dr. Georg Scheffers. I. Mit 107 Figuren. Dritte, verbesserte Auflage. XII, 482 Seiten. 1923 . . . . . RM. 13.—, geb. RM. 14.50
II. Mit 110 Figuren. Dritte, verbesserte Auflage. XI, 582 Seiten. 1922. RM. 15.—, geb. RM. 16.50

Theorie der Raumkurven und krummen Flächen. Von Oberstudiendirektor Prof. Dr. V. Kommerell in Tübingen und Prof. Dr. K. Kommerell in Tübingen. I: Krümmung der Raumkurven und Flächen. Vierte Auflage. Mit 38 Figuren. 205 Seiten. 1931. (Göschens Lehrbücherei Bd. 20) Geb. RM. 10.—
II: Kurven auf Flächen. Spezielle Flächen. Theorie der Strahlensysteme. Vierte Auflage. Mit 22 Figuren. 194 Seiten. 1931. Geb. RM. 10.—

Lehrbuch der darstellenden Geometrie. Von Dr. Karl Rohn, Geh. Rat, weiland Professor an der Universität Leipzig, und Dr. Erwin Papperitz, Geh. Rat, Professor an der Bergakademie in Freiberg i. Sa. Drei Bände. Groß-Oktav. I. Orthogonalprojektion. Vielflache, Perspektivität ebener Figuren, Kurven, Zylinder, Kugel, Kegel, Rotations- und Schraubenflächen. Vierte, erweiterte Auflage. XX, 502 Seiten. Mit 351 Figuren. Neudruck 1932. . . . . Geb. RM 18.90
II. Axonometrie, Perspektive, Beleuchtung. Vierte, umgearbeitete Auflage. VI, 194 Seiten. Mit 118 Figuren. Neudruck 1932. Geb. RM. 8.55
III. Kegelschnitte, Flächen zweiten Grades, Regel-, abwickelbare und andere Flächen. Flächenkrümmung. Vierte, unveränderte Auflage. X, 334 Seiten. Mit 157 Figuren. 1923 . . . . . Geb. RM. 12.—

Darstellende Geometrie. Von Theodor Schmid, o. ö. Professor an der Technischen Hochschule in Wien. I. Teil: Eckige Körper, Kugel, Zylinder, Kegel, Plankurven und Raumkurven mit den zugehörigen Torsen im Normalrißverfahren und in orthogonaler Axonometrie. Dritte Auflage. Mit 170 Figuren. 283 S. 1922. (Samml. Schubert Bd. 65) Geb. RM. 6.—
II. Teil: Schiefe und zentrale Projektion. Dreh-, Rohr-, Schrauben- und Regelflächen. Geländedarstellung, Kartenprojektion, Nomographie. Zweite Auflage. Mit 163 Fig. 340 S. 1923. (Samml. Schubert Bd. 66) Geb. RM. 7.50

Die Lehre von der Zentralprojektion im vierdimensionalen Raume. Von Dr. H. de Vries, Professor an der Universität zu Amsterdam. Mit 25 Figuren. Lex.-8° 178 S. 1905 . . . . . RM. 3.—

Angewandte Potentialtheorie in elementarer Behandlung. I. Bd. Von Professor E. Grimsehl. Mit 74 Fig. [Sammlung Schubert Bd. XXXVIII.] Gr. 8° VII, 219 S. 1905 . . . . . Geb. RM 7.40

Methoden der praktischen Analysis. Von Professor Dr. Fr. A. Willers. Mit 132 Figuren. 344 Seiten. 1928. (Göschens Lehrbücherei Bd. 12) RM. 20.—, geb. RM. 21.50

Der Band gibt dem Mathematiker einen Einblick in die Anwendungsmöglichkeiten der Methoden und macht den Naturwissenschaftler und Ingenieur mit den theoretischen Grundlagen bekannt.

Wahrscheinlichkeitsrechnung für Nichtmathematiker. Von Dr. Karl Dörge, o. Professor an der Universität Köln, unter Mitwirkung von Hans Klein. Groß-Oktav. 113 Seiten. 1939 . . . . . Geb. RM. 6.—

Ballistik. Von Professor Dr. Theodor Vahlen. Mit 53 Abbildungen. Groß-Oktav. XII, 231 Seiten. 1922 . . . . . RM. 9.—, geb. RM. 10.—

MINERVA

JAHRBUCH DER GELEHRTEN WELT

Herausgegeben von Dr. GERHARD LÜDTKE

33. Jahrgang

Abteilung:

Universitäten und Fachhochschulen

Band I: **Europa**

Oktav. 1330 Seiten. 1938. Gebunden RM. 42.—

Band II: **Die außereuropäischen Hochschulen**

Oktav. 1029 Seiten. 1938. Gebunden RM. 38.—

32. Jahrgang

Abteilung:

Forschungsinstitute, Observatorien, Bibliotheken, Archive, Museen, Kommissionen, Gesellschaften

Oktav. 1765 Seiten. 1937. Gebunden RM. 58.—

Weltkalender der Gelehrten

Herausgegeben von Dr. GERHARD LÜDTKE

Redaktionelle Leitung Dr. FRIEDRICH RICHTER

Oktav. VIII. 1481 Seiten. 1936. Gebunden RM. 45.—

WALTER DE GRUYTER & CO. / BERLIN W 35

Buchdruckerei Otto Regel GmbH., Leipzig

Co lekcja
a 25. 9 —

3365
Jk

fl. 9 3/32
19/X 195