

Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung.

Von DIETRICH MAHNKE in Stade.

Die LEIBNIZhandschriften in der Kgl. Bibliothek zu Hannover bergen noch immer ungehobene Schätze. Allerdings könnte man fast versucht sein, auf diese ein Wort anzuwenden, das LEIBNIZ manchmal von der scholastischen Philosophie gebrauchte: „aurum latere in stercore“. Denn die wertvollsten Entdeckungen stehen hier oft auf abgerissenen Papierfetzen und Briefumschlägen oder auf den Rändern anderer weniger wertvollen Entwürfe, bei deren Niederschrift ihm die guten Gedanken gekommen sind. Außerdem enthalten die Handschriften nicht nur die endgültigen Ergebnisse des Nachdenkens, sondern auch die sämtlichen Vorüberlegungen und Nebenrechnungen, ferner alle Umwege, auf denen der Entdecker das erste Mal nur mühsam zum Ziele gelangt ist, ja selbst falsche Schlüsse und vergebliche Versuche, die LEIBNIZ hat abschließen müssen mit einem: „res distinctius examinanda“ oder „hoc accuratius tractandum“. ¹⁾

1) So z. B. Math. Vol. III, 26, Blatt 11, Rückseite. Vol. IIIB, 11, Blatt 30, Rückseite. — In dieser Weise zitiere ich die hannoverschen LEIBNIZhandschriften zur Mathematik. Sie können unter diesen Nummern an Ort und Stelle sofort aufgefunden werden. Vgl. BODEMANN, *Die LEIBNIZhandschriften der Kgl. Bibliothek zu Hannover*, Hannover 1895. Die Zitate sind nach bestem Wissen und Willen buchstabengetreu. Nur die Inkonsequenz der großen Anfangsbuchstaben und der Interpunktion habe ich beseitigt. Die Klammern {} schließen spätere Zusätze LEIBNIZENS ein, die Klammern [] dagegen bedeuten, daß das Eingeschlossene von LEIBNIZ nachträglich als ungültig eingeklammert oder durchstrichen ist. (Diese Bezeichnungsart stammt von COUTURAT.) Ich gebrauche ferner folgende Abkürzungen:

CANTOR, *Vorl.* III² = M. CANTOR, *Vorlesungen über Geschichte der Mathematik*, Bd. III, 2. Auflage, Leipzig 1901.

TROPFKE, *Gesch.* = J. TROPFKE, *Geschichte der Elementarmathematik*, Leipzig 1902/3. LEIBNIZENS *Math. Schr.* III. VII = LEIBNIZENS *mathematische Schriften*, herausg. von C. I. GERHARDT, Bd. III, VII, Halle 1855/63.

COUTURAT, *Log.* = L. COUTURAT, *La logique de LEIBNIZ*, Paris 1901.

COUTURAT, *Opusc.* = L. COUTURAT, *Opuscules et fragments inédits de LEIBNIZ*, Paris 1903.

Aber unter all diesem Wust liegen Geistesschätze begraben, die namentlich für den Historiker der Mathematik von einzigartigem Werte sind. Denn sie ermöglichen die auf den Tag genaue Zeitbestimmung mancher Entdeckung, die für die Entwicklung der Wissenschaft von größter Wichtigkeit geworden ist. Aber mehr — sie geben uns Gelegenheit, nicht nur die Phylogenese, sondern sogar die Ontogenese der mathematischen Erkenntnis zu erforschen. Denn wie der Stammesgeschichte der Organismen die Entwicklung des Einzelwesens entspricht, so auch der Geschichte der Wissenschaft im großen die Entstehung der Einzelerkenntnis im Geiste des individuellen Forschers. Die LEIBNIZHANDSCHRIFTEN nun verschaffen uns die Grundlagen einer solchen geistigen Embryologie, weil in ihnen alle einzelnen Entwicklungsstadien der großen Entdeckungen im Geiste des genialen Forschers von der ersten lustvollen Empfängnis an durch alle mühsamen Jahre des allmählichen Reifens hindurch erhalten sind. Wohl nirgends sonst in der Welt bietet sich eine gleich gute Gelegenheit, die Psyche eines so bedeutenden Mathematikers aus unmittelbarer Nähe bei der Arbeit zu belauschen und das „embryonale“ Werden von Geistesschöpfungen zu studieren — ein Studium, das noch um vieles interessanter ist als die Erforschung des ähnlichen Wunders auf biologischem Gebiete.

Ich werde im folgenden ein Beispiel näher ausführen, auf das ich beim Studium der LEIBNIZHANDSCHRIFTEN für einen anderen Zweck (die Geschichte der philosophischen Wahrscheinlichkeitslehre) zufällig gestoßen bin, nämlich die LEIBNIZSCHE WIEDERENTDECKUNG und Weiterbildung des FERMATSCHEN SATZES, nach dem $a^{p-1} \equiv 1 \pmod{p}$ immer dann ist, wenn p eine Primzahl und a eine zu p prime ganze Zahl ist.

Bekanntlich hat FERMAT diesen Satz am 18. Oktober 1640 an seinen Freund FRÉNICLE geschrieben, doch — wie es überhaupt seine Art war — ohne seinen Beweis mitanzugeben.¹⁾ Durch den Druck dieses Briefes in FERMATS Werken wurde der Satz, aber immer noch ohne Beweis, in der wissenschaftlichen Welt bekannt. Der erste Mathematiker, der einen Beweis veröffentlichte, war EULER (1736).²⁾ Doch behauptete 1752 JOHANN SAMUEL

1) „Dequoy je vous enverrois la demonstration, si je n'apprehendois d'être trop long.“ *Varia opera mathematica D. PETRI DE FERMAT*, Tolosae 1679, p. 163. Vgl. *Oeuvres DE FERMAT* 2, Paris 1894, p. 209.

2) EULER erwähnte den FERMATSCHEN SATZ zuerst in den *Observationes de theoremate quodam FERMATIANO aliisque ad numeros primos spectantibus*; *Commentarii Academiae scientiarum Petropolitanae* 6, 1732/33, 103—107, ohne aber einen Beweis für ihn geben zu können. Sein erster, dem LEIBNIZSCHEN ähnlicher Beweis findet sich in der Abhandlung *Theoremata quorundam ad numeros primos spectantium demonstratio*; *Comm. Ac. sc. Petr.* 8, 1736, 141—146. Einen zweiten, eigentlich zahlentheoretischen Beweis gab er dann in den *Theoremata circa residua ex divisione potestatum relicta*; *Novi Comm. Ac. sc. Petr.* 7, 1758/9, 49—82, und gelangte

KÖNIG in seinem Streite mit MAUPERTUIS (dem er zu LEIBNIZENS Gunsten die erste Entdeckung des Prinzips der kleinsten Wirkung bestritt), jene „démonstration d'une certaine propriété des nombres premiers, de laquelle il (EULER) se croit seul et premier inventeur“, finde sich schon bei LEIBNIZ. Er stützte sich dabei auf ein eigenhändiges Schriftstück von diesem, das sich in seinen Händen befand.¹⁾ Auch GAUSS kam im Artikel 50 seiner *Disquisitiones arithmeticae* (1801) auf die von KÖNIG behauptete Priorität LEIBNIZENS zu sprechen, ließ aber die Frage, da nichts Gedrucktes vorlag, unentschieden.

Erst 1894 stellte G. VACCA²⁾, indem er auf eine Stelle der inzwischen gedruckten LEIBNIZschen Abhandlung *Nova algebrae promotio*³⁾ hinwies, endgültig fest, daß LEIBNIZ tatsächlich den EULERSchen Beweis des FERMATschen Satzes schon besessen habe. Fünf Jahre später machte VACCA²⁾ auch noch auf ungedruckte Handschriften der Kgl. Bibliothek in Hannover aufmerksam, aus denen sich „il processo della ideazione nella mente di LEIBNIZ“ erkennen lasse, während aus der von GERHARDT gedruckten Abhandlung nicht ersichtlich werde, auf welchem Wege LEIBNIZ gewissermaßen ohne Kraftanstrengung zu dem Resultate gelangt sei, zu dem EULER später einen so mühsamen Weg habe gehen müssen. VACCA nannte dabei die Handschriften Math. Vol. III B 11 und Vol. III B 17, Blatt 3. Das letztere Blatt, datiert vom 1. Juni 1683, war das zeitlich früheste, das er gefunden hatte.

Doch auch durch diese Feststellungen VACCAS war noch nicht alle Unklarheit beseitigt. Insbesondere war noch nicht entschieden, ob LEIBNIZ den Satz, unabhängig von FERMAT, völlig neu gefunden oder nur durch einen Beweis bereichert habe. Da die älteste VACCA bekannte Handschrift, die sich auf den Satz bezieht, aus dem Jahre 1683 stammt, FERMATS Werke aber, die LEIBNIZ bei seinem damaligen großen Interesse für Zahlentheorie sicher studiert hat, schon 1679 erschienen sind, so mußte man annehmen, daß der Satz von FERMAT übernommen sei. Andererseits aber machte CANTOR⁴⁾ darauf aufmerksam, daß LEIBNIZ sich in der *Nova algebrae promotio* auf den Satz viel zugute tue, weil er etwas den Analytikern bisher Unbekanntes enthalte: eine allgemeine Primzahlenformel, und schloß daraus — mit Un-

endlich in den *Novi Comm. Ac. sc. Petr.* 8, 1760/1, 74 u. folg., zu der nach ihm genannten Verallgemeinerung: $a^{q(n)} \equiv 1 \pmod{n}$ für beliebig zusammengesetzte Zahlen n und alle zu n primen Zahlen a .

1) JOH. SAM. KÖNIG, *Appel au public*, Leyden, 1. Aufl. 1752, p. 104; 2. Aufl. 1753, p. 106.

2) G. VACCA, *Intorno alla prima dimostrazione di un teorema di FERMAT*; *Bibl. math.* 1894, 46 — 48. Derselbe, *Sui manoscritti inediti di LEIBNIZ*; *Bollettino di bibliogr. e storia delle sc. mat.*, 2, 1899, p. 113. Vgl. ferner COUTURAT, *Log.* 478, 499, 500; *Opusc.* 575.

3) LEIBNIZENS *Math. Schr.* VII, 180, 181.

4) CANTOR, *Vorl.* III², 331.

recht, wie wir sehen werden —, daß LEIBNIZ VON FERMATS Priorität nichts gewußt habe.

Um diese Unklarheit zu beseitigen und gleichzeitig den „Gang der Ideenentwicklung“ im Geiste des großen Mathematikers und damit die Psychologie einer mathematischen Entdeckung aufzuhellen, habe ich einen großen Teil der hannoverschen Handschriften durchgesehen. Ich bin dabei zu folgenden Ergebnissen gekommen.

LEIBNIZ hat einige spezielle Fälle des FERMATSchen Satzes, nämlich $a^2 \equiv 1 \pmod{3}$ und $a^4 \equiv 1 \pmod{5}$, schon im Januar 1676 aus den Formeln der figurierten Zahlen bewiesen. Die Verallgemeinerung dieser Ableitung würde auf die Betrachtung des Ausdruckes $(x+1)(x+2)\cdots(x+p-1)$ führen, mit dessen Hilfe 1771 (1773) LAGRANGE den FERMATSchen gleichzeitig mit dem WILSONSchen Satze bewiesen hat. In den Jahren 1677—79 hat LEIBNIZ die periodischen Dual-, Trial-, . . . Dezimalbrüche in ihrer Beziehung zu den Resten der Potenzen von $2, 3 \dots 10 \pmod{n}$ betrachtet und daraus einen Satz gewonnen, der sich in der GAUSSischen Bezeichnungsweise so ausdrücken läßt: Es kann immer ein $k < n$ gefunden werden, so daß $a^k \equiv 1 \pmod{n}$ ist. Später hat er diesen Satz dahin berichtigt, daß er für die Primzahlen n gilt. Daß man bei Primzahlmodul immer $k = n - 1$ setzen darf, hat er zuerst am 12. September 1680 erkannt und aus den sog. NEWTONSchen Potenzsummenformeln, die er damals schon selbständig gefunden hatte, bewiesen. Einen weiteren einfachen Beweis des FERMATSchen Satzes für die Basis 2 aus dem binomischen Lehrsatz hat LEIBNIZ vielleicht noch an demselben Tage entdeckt. Dagegen ist der durch VACCA bekannt gewordene Beweis für beliebige a aus dem polynomischen Lehrsatz wohl erst einige Jahre später von LEIBNIZ durchgeführt worden, wenn ihm auch der polynomische Lehrsatz selbst schon seit Oktober 1676 bekannt war.

Aus dem binomischen Lehrsatz hat LEIBNIZ auch die Umkehrung des FERMATSchen Satzes zu beweisen gesucht: Wenn $2^p - 1 \equiv 1 \pmod{p}$ ist, so ist p Primzahl. Der Beweis ist aber unzureichend, und der Satz ist falsch, wie schon das Beispiel $2^{11 \cdot 31} - 1 \equiv 1 \pmod{11 \cdot 31}$ zeigt. Ja, es gibt sogar zusammengesetzte Zahlen n , für die $a^{n-1} \equiv 1 \pmod{n}$ bei jeder zu n primen Basis a ist; dies ist, wie ich zur Prüfung der LEIBNIZschen Behauptung festgestellt habe, z. B. bei $n = 3 \cdot 11 \cdot 17$ wirklich der Fall.

Einen anderen Fehler hat LEIBNIZ selbst bald berichtigt. Während er 1680 gemeint hatte, wenn p eine Primzahl sei, so sei $k = n - 1$ der kleinste Exponent, für den $a^k \equiv 1 \pmod{p}$ werde, hat er bald erkannt, daß k ebensoviel ein echter Teiler von $n - 1$ sein könne. Vielleicht ist ihm jetzt bei der genaueren Formulierung des Satzes das Studium der Werke FERMATS von Nutzen gewesen, aus denen er den in Frage stehenden Satz — ich vermute um 1681 — exzerpiert hat, wie die noch vorhandenen Auszüge beweisen.

Indem er mit dem von FERMAT stammenden Satze seine Umkehrung verband, meinte LEIBNIZ die lange gesuchte „definitio realis seu aequatio generalis numeri primitivi“ oder, wie er auch sagt, die „proprietas seu nota reciproca primitivi“, die notwendige und hinreichende Bedingung der Primzahlen, gefunden zu haben. Aus dieser fälschlich für genügend gehaltenen Gleichung, $2^{p-1} = mp + 1$, hat er dann, indem er 1682/3 seinen Exponentialkalkül auf ihre Behandlung anwandte, eine ziemlich einfache Methode zur Erkennung einer Zahl als Primzahl abgeleitet, in die aber leider der Irrtum der Voraussetzung mit eingegangen ist. Seine Methode läßt ein gewandtes Rechnen mit Kongruenzen, insbesondere mit Potenzresten, erkennen und rührt schon an die Sätze, auf die später das Rechnen mit Indices in der Zahlentheorie gegründet worden ist.

Die eben geschilderten Tatsachen ergeben sich aus den folgenden Handschriften der Kgl. Bibliothek zu Hannover, die ich, so gut es geht, in historischer Folge zusammenstelle:

1. Math. Vol. IV, 17, Blatt 7. Ouverture nouvelle de nombres multiples, et des diviseurs des puissances. 3. Januar 1676. (COUTURAT, *Opusc.* 587.)

2. III, B, 14, Blatt 1. De numero jactuum in tesseris. Proposuit mihi dux ROANNESIUS. Januar 1676.

3. XII, 2, Blatt 3. ($y^3 - y, y^5 - y$)

4. XII, 1, Blatt 39. Conversation avec MONS. DE MARIOTTE touchant les nombres. 10. Februar 1676.

5. IV, 11. Conspectus calculi. (LEIBNIZENS *Math. Schr.* VII, 83—100.)

6. IH, B, 15, Blatt 6. 12. Februar 1676. Anfang April 1676.

$$(p = 6n \pm 1)$$

7. 8. IV, 17, Blatt 1, 2. Numeri primi eorumque genesis mira. 6., 7. September 1677. ($p = 6n \pm 1$)

9. III, 24. Logistica decimalis. 12. November 1677.

10. IV, 17, Blatt 3. De numeris primitivis. Dezember 1677.

$$(p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots \pm 1.)$$

11. III, 24, Blatt 6. Reductio ad decimales. Februar 1678.

12. XII, 2, Blatt 4. De decimalibus vel similibus et earum periodo inveniendi. (Auf einem Briefumschlage: Monsieur de LEIBNITZ A Hannover.)

13. III, 4, Blatt 14. Formarum reductio ad simplices. 12. September 1680.

14. IV, 17, Blatt 9. ($2^k \equiv 1 \pmod{n}, k < n$) Blatt 8. ($2^2 - 2, 2^{2-1} - 1$)

15. III, B, 17, Blatt 2. Ex M. JOH. WILH. PAULI Philintri (?) Lips. de num. perf. Lips. 1678.

16. III, B, 17, Blatt 1. Demonstratio de numero perfecto in progressionem binaria.

17. XIV, 2, Blatt 20—26. Auszüge aus FERMATS „Omnia (?) opera mathematica“, Tolosae 1679.

18. III, B, 12. De numeri primitivi nota. (Erster Beweisversuch der Umkehrung des FERMATSchen Satzes.)

19. III, 26, Blatt 7 ff., 11 ff. De primitivis ex tabula combinatoria (zwei Entwürfe). Dezember 1681.

20. III, 26, Blatt 1—6. De primitivis et divisoribus ex tabula combinatoria. (*LEIBNIZENS Math. Schr.* III, 109—113.)

21. III, B, 11, Blatt 9. (Reste der Potenzen von 2 (mod. 31))

22. III, B, 11, Blatt 7. (Logarithmen zur Basis 2.)

23. III, B, 15, Blatt 5

24. III, B, 11, Blatt 18 } $(2^{y-1} - yz)$

25. III, B, 11, Blatt 21. $n - 2! \equiv 1 \pmod{p}$.

26. III, B, 15, Blatt 7. Agnoscere primitivos. Juni 1682.

27. III, B, 17, Blatt 6. Agnoscere primitivos. (Neunerreste der Potenzen von 2.)

28. III, B, 11, Blatt 30. (Differenzlogarithmen.)

29. III, B, 17, Bl. 3. Aeqvatio primitivi. Hic tandem arcanum illud detectum videtur. 1. Juni 1683.

30. III, B, 11, Blatt 4. (Beweis von $a^{p-1} \equiv 1 \pmod{p}$). Logarithmische Beziehung zwischen Potenzen und Potenzresten.)

31. 32. III, B, 11, Blatt 5 und 6. Blatt 14. (Über $2^n - 1$ und seine Teiler.)

33. III, B, 15, Blatt 1. G. G. L. Novus aditus ad incognita hactenus mysteria numerorum.

34. III, B, 11, Blatt 1, 28. Inquisitio in numeros primitivos et divisorum divisores.

35. 36, 37, III, B, 11, Blatt 2, 8, 27. (Nähere Ausführungen zu 34.)

38. III, 25, Blatt 1 ff. De periodis decimalibus. Insignia inventa. 12. Januar 1687.

39. III, 25, Blatt 10. De periodis fractionum decimalium et numerorum primitivorum analysi (?). Januar 1687.

40. IV, 5. Nova algebrae promotio. (*LEIBNIZENS Math. Schr.* VII, 154—189.)

Auf den FERMATSchen Satz kam LEIBNIZ zuerst bei Gelegenheit kombinatorischer Untersuchungen. War doch die Kombinationslehre eins der wenigen Gebiete der Mathematik, die schon dem jungen Studenten der Philosophie und Jurisprudenz in Leipzig vertraut geworden waren. Durch das Studium BISTERFELDS¹⁾ war ihm nämlich der logische und metaphysische

1) JOH. HENR. BISTERFELDII *Philosophiae primae seminarium*, Leyden 1657. *Elementorum logicorum libri tres*. *Phosphorus catholicus*, Leyden 1657. Auf die Bedeutung

Wert dieses Teiles der Arithmetik klar geworden, und er hatte sich deshalb in seiner Schrift *De arte combinatoria* (1666) bemüht, die Kombinationslehre als eine neue Logik der Erfindung fortzubilden.

Während seines Pariser Aufenthaltes (März 1672 bis Okt. 1676) dagegen begann ihn die Mathematik auch um ihrer selbst willen zu interessieren. Schon 1672 entdeckte er die Summenformel für die 3. Potenzen der aufeinanderfolgenden ganzen Zahlen¹⁾ mit Hilfe der von ihm sogenannten „erzeugenden Differenzen“, erfuhr aber am 2. Februar 1673 in London durch PELL, den er bei BOYLE getroffen hatte, daß ihm in der Anwendung dieser Methode REGNAUD in Lyon zuvorgekommen sei, und daß dessen Entdeckung sogar schon in dem Buche von MOUTON, *Observationes diametrorum solis et lunae apparentium* (1670), gedruckt sei.²⁾ Diese Erfahrung wurde für LEIBNIZ der Anlaß zum sorgfältigen Studium der vorhandenen mathematischen Literatur. Nach Paris zurückgekehrt, setzte er sich mit dem dort lebenden HUYGENS in Verbindung, um durch diesen in die neuesten Fortschritte der Mathematik eingeführt zu werden.

Auf dem Gebiete der Kombinationslehre insbesondere studierte er eingehend PASCALS *Traité du triangle arithmétique*, der 1654 geschrieben, freilich erst seit 1665 im Buchhandel erhältlich war. LEIBNIZ machte sich dessen Hauptsatz völlig zu eigen, den man in der heute üblichen Ausdrucksweise kurz etwa so aussprechen kann: Die Anzahl der Kombinationen von n Elementen zur k^{ten} Klasse ohne Wiederholung ist identisch mit drei anderen Zahlen, nämlich 1. dem $(k+1)^{\text{ten}}$ Koeffizienten der n^{ten} Potenz eines Binoms, 2. dem $(n-k+1)^{\text{ten}}$ Gliede der einfachsten arithmetischen Reihe k^{ter} Ordnung, 3. der $(n-k+1)^{\text{ten}}$ figurierten Zahl der $(k+1)^{\text{ten}}$ Ordnung. LEIBNIZ nannte diese Zahl die der „con k maisons dans n “. Er schrieb ihre Formel:

$$\frac{n \cap n-1 \cap n-2 \text{ etc. } \cap n-k+1}{1 \cap 2 \cap 3 \text{ etc. } \cap k}$$

und gab dem PASCALSchen Dreieck, um diese Zahl aus ihm leichter ablesen zu können, eine passendere Anordnung³⁾:

dieses Kombinatorikers in Leyden für die philosophische Entwicklung LEIBNIZENS hat zuerst W. KABITZ, *Die Philosophie des jungen LEIBNIZ*, Heidelberg 1909, S. 6–8, 16, hingewiesen.

1) Daß $\sum_1^n (x^n) = \left(\sum_1^n x\right)^2$ ist, wußten wahrscheinlich schon die griechischen Mathematiker, jedenfalls die römischen Agrimensoren und die indischen Mathematiker des Mittelalters. Über die spätere Geschichte des Satzes vgl. P. TANNERY, *Bibl. Math.* 3., 1902, S. 257–258. 1672 aber wußte LEIBNIZ weder etwas von diesen Vorgängern noch von PASCALS allgemeiner Summationsmethode (*Potestatum numericarum summa*).

2) Vgl. GUHRAUER, *LEIBNITZ. Eine Biographie*. 2. Aufl., Breslau 1846, I, 126.

3) Handschrift 2. Ebenso *LEIBNIZENS Math. Schr.* VII, 101. Eine der LEIBNIZschen ähnliche Anordnung, doch ohne Nummerierung der Zeilen und Spalten, hatte schon

PASCALSches Dreieck.

	1	2	3	4	5	6	7	<i>m</i>
1	1	1	1	1	1	1	1	
2	1	2	3	4	5	6		
3	1	3	6	10	15			
4	1	4	10	20				
5	1	5	15					
6	1	6						
7	1							
<i>y</i>								

Bipyramidaux.
Triangulo-Pyramidaux.
Bitriangulaires.
Pyramidaux.
Triangulaires.

LEIBNIZSche Anordnung.

	0	1	2	3	4	5	6	<i>k</i>
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
<i>n</i>								

Unio.
Binio.
Ternio.
Quaternio.
Quinio.
Senio.

Die LEIBNIZSche Anordnung ist am Platze, wenn es sich um Kombinationen oder Binomialkoeffizienten handelt, die PASCALSche dagegen, wenn figurierte Zahlen oder Glieder von arithmetischen Reihen berechnet werden sollen. Im letzteren Falle spricht man den Hauptsatz besser so aus: Die y^{te} figurierte Zahl der m^{ten} Ordnung ist identisch mit 1. dem y^{ten} Gliede der einfachsten arithmetischen Reihe $(m-1)^{\text{ter}}$ Ordnung, 2. dem Koeffizienten des m^{ten} Gliedes der $(y+m-2)^{\text{ten}}$ Potenz eines Binoms und 3. der Anzahl der Kombinationen von $(y+m-2)$ Elementen zur $(m-1)^{\text{ten}}$ Klasse ohne Wiederholung. Diese Zahl schreibt LEIBNIZ in der Form:

$$\frac{y+m-2}{1} \cdot \frac{y+m-3}{2} \text{ etc. } \cdot \frac{y}{m-1}$$

Indem LEIBNIZ diese PASCALSchen Entdeckungen geistig verarbeitete und mit seiner Methode der „erzeugenden Differenzen“ vereinigte, gewann er eine Reihe von arithmetischen Erkenntnissen. Seine Methode reichte doch weiter als die des REGNAUD. Sie befähigte ihn nämlich, alle Reihen von Brüchen zu addieren, in deren Zähler die Einheit und in deren Nenner figurierte Zahlen beliebiger Ordnung stehen. Solche Reihen nannte LEIBNIZ harmonische und stellte zu ihrer Addition 1673 ein „harmonisches Dreieck“ auf, entsprechend der Addition der figurierten Zahlen durch das PASCALSche Dreieck.¹⁾ Auch solche Reihen nannte LEIBNIZ noch harmonische, die „durch einen Sprung“ etwa aus der Reihe $\frac{1}{1}, \frac{1}{3}, \frac{1}{5}, \frac{1}{7} \dots$ hervorgehen, näm-

STIFEL, *Arithmetica integra* (1544), Bl. 46^r, zusammengestellt, um mit ihrer Hilfe höhere Wurzeln auszuziehen. Später benutzte JAKOB BERNOULLI, *Ars conjectandi* (Basel 1713), p. 87, die gleiche Anordnung wie LEIBNIZ für den gleichen Zweck, ließ aber unpraktischerweise k und n mit 1 statt mit 0 beginnen.

1) Erster Entwurf Math. III B 10 mit der Bemerkung: Hic primum cepi invenire. Ferner III B 18 und VIII 27 Blatt 1. 2, Blatt 1 mit der Notiz: Origo inventionis trianguli harmonici anno 1673. HUGENIUS mihi proposuerat summam fractionum triangularium inveniendam ..., Blatt 2 mit dem Datum: Febr. 1676. Vgl. COUTURAT, *Opusc.* 589.

lich $\frac{1}{1}, \frac{1}{5}, \frac{1}{9} \dots$ und $\frac{1}{3}, \frac{1}{7}, \frac{1}{11} \dots$. Subtrahiert man die zweite Reihe von der ersten, so entsteht die auch heute noch sogenannte LEIBNIZsche Reihe: $\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$, deren Summe LEIBNIZ 1674 als gleich $\frac{\pi}{4}$ erkannte.

Ferner führte LEIBNIZ 1674 den Begriff der „divulsiones“ ein¹⁾, d. h. die Variationen zu bestimmten Summen oder, umgekehrt ausgedrückt, die Zerfällung einer Zahl in eine bestimmte Anzahl von Summanden. Z. B. gibt es 3 divulsiones der Zahl 3, nämlich die Zahl selbst, ihre „discerptio“, $2 + 1$ und ihre „triscerptio“, $1 + 1 + 1$. Ebenso gibt es 5 divulsiones der Zahl 4, nämlich die Zahl selbst, ihre „discerptiones“, $3 + 1, 2 + 2$, ihre „triscerptio“, $2 + 1 + 1$ und ihre vierfache Zerfällung, $1 + 1 + 1 + 1$. Von 5 gibt es 7 divulsiones, von 6 gibt es 11, so daß man meinen könnte, hier entstünden die Primzahlen. Doch die Anzahl der Zerfällungen von 7, die 15 beträgt, erweist diesen Schluß als „exemplum memorabile fallentis inductionis“ (Math. Vol. XII 1 Blatt 18). Wir erkennen hier das Bestreben LEIBNIZENS, die Kombinatorik zur Zahlentheorie in Beziehung zu setzen. An dieser Stelle war allerdings seine Bemühung vergeblich, aber später werden wir wertvolle Früchte dieser Verbindung beobachten können.

LEIBNIZ gebrauchte die „divulsiones“ außer bei der Multiplikation von Polynomen vor allem bei der Behandlung der Ausdrücke, denen er den — heute in etwas anderer Bedeutung gebrauchten — Namen „Formen“ gegeben hat. Eine „Form“ entsteht nach ihm, wenn in irgend einem eingliedrigen Ausdruck, etwa ab^3c^2 , für a, b, c der Reihe nach alle Kombinationen von n Elementen $a, b, c \dots n$ zur k^{ten} (hier 3.) Klasse gesetzt, die Exponenten dagegen nicht verändert werden und wenn schließlich alle so entstandenen Ausdrücke addiert werden: $ab^3c^2 + ab^3d^2 + \dots + bc^3d^2 + \dots$. LEIBNIZ kürzt diesen Ausdruck folgendermaßen ab: $a\ddot{b}^3c^2$, während man heute $\sum_1^n ab^3c^2$ schreibt.²⁾ Von jedem Grade gibt es nach LEIBNIZ so viel Formen wie „divulsiones“ des Exponenten, der den Grad angibt:

1. Grad $a (= a + b + c \dots)$
2. Grad $a\ddot{a}b (= ab + ac + ad \dots + bc + bd \dots)$
3. Grad $a\ddot{a}^3, a\ddot{a}^2b, a\ddot{a}bc.$

Von besonderer Wichtigkeit sind die „formae simplices“, die heute sogenannten elementaren symmetrischen Funktionen: $a, a\ddot{b}, a\ddot{b}c$ usw. Wenn

1) Math. Vol. IV 2: Specimen de divulsionibus aequationum ... Blatt 3 datiert 2. Sept. 1674. Math. Vol. XII 1, Blatt 15: Regula discerptionum et triscerptionum universalis. Blatt 16: Formae combinatoriae (20. Okt 1675). Blatt 18: De numero formarum (Febr. 1676). Vol. III B 14, Blatt 4: Regula discerptionum universalis.

2) Vgl. die in Anmerkung 1) zitierten Handschriften, ferner Math. XII 2, Blatt 139 u. a. LEIBNIZENS Math. Schr. VII 88 (Conspectus calculi), 178 (Nova algebrae promotio).

man nämlich unter $a, b, c \dots n$ die Wurzeln einer Gleichung n^{ten} Grades versteht, so ist die elementare symmetrische Funktion k^{ten} Grades identisch mit dem Koeffizienten von x^{n-k} in der Gleichung, multipliziert mit $(-1)^k$, vorausgesetzt, daß der Exponent von x^n gleich 1 gemacht ist. Das hatte LEIBNIZ von VIÈTE und DESCARTES gelernt, wie die ausdrückliche Anführung dieser großen Algebraiker zeigt. Er überlegte nun, ob es nicht auch möglich sei, daß andere symmetrische Funktionen der Wurzeln rationale Werte annehmen, wenn auch die Wurzeln irrational seien, wie dies ja bei den elementaren symmetrischen Funktionen der Fall ist. Er fand, daß dasselbe auch bei den Summen der Potenzen der Wurzeln eintrete, da man diese durch die elementaren symmetrischen Funktionen rational ausdrücken könne. Im September 1678 spätestens¹⁾ war er im Besitz der folgenden Formeln:

$$\begin{aligned} a^1 &= a \\ a^2 &= (a)^2 - 2(ab) \\ a^3 &= (a)^3 - 3(a) \cdot (ab) + 3(abc) \\ a^4 &= (a)^4 - 4(a)^2(ab) + 4(a)(abc) + 2(ab)^2 - 4(abcd) \\ a^5 &= (a)^5 - 5(a)^3(ab) + 5(a)^2(abc) + 5(a)(ab)^2 \\ &\quad - 5(a)(abcd) - 5(ab)(abc) + 5(abcde) \end{aligned}$$

Damit hatte LEIBNIZ die von ALBERT GIRARD²⁾ zuerst abgeleiteten Formeln für die 1. bis 4. Potenz unabhängig von ihm wieder entdeckt und auf höhere Potenzen ausgedehnt. Man pflegt diese Formeln die NEWTONSchen Potenzsummenformeln zu nennen. NEWTON hat sie 1681 in seinen Vorlesungen vorgetragen, und WHISTON hat sie 1707 in der Ausgabe von NEWTONS *Arithmetica universalis* veröffentlicht. Die angegebenen LEIBNIZ-handschriften zeigen, daß, wenn man die Formeln nicht nach GIRARD benennen will, LEIBNIZ fast denselben Anspruch auf sie hat wie NEWTON.

Mit der Lehre von den „divulsiones“ und „formae“ hängt auch eine weitere Entdeckung zusammen, die LEIBNIZ in der gleichen Zeit machte, die des polynomischen Lehrsatzes. Denn offenbar ergibt sich bei der Erhebung eines Polynoms in die n^{te} Potenz eine Summe von Formen n^{ten} Grades, und es handelt sich nur um die Feststellung der Häufigkeiten des Vorkommens jeder Form, d. h. der Polynomkoeffizienten. COUTURAT³⁾ ver-

1) Math. Vol. III, 3: De rationali parte potestatum a radicibus aequationum, darin Blatt 4 vom Sept. 1678, enthaltend: Summa radicum, quadratorum a radicibus, cuborum, qqtorum, surdesolidorum, quadratocuborum. Math. Vol. III, 4: Aequationum resolutio generalis tentata, darin Blatt 14 vom 12. Sept. 1680: Formarum reductio ad simplices. Auf diesem Blatte ist LEIBNIZ der erste Beweis des FERMATSchen Satzes gelungen.

2) *Invention nouvelle en l'algèbre*, Amsterdam 1629; Neudruck Leyden 1884.

3) *Logique* 496.

mutet wohl mit Recht, daß LEIBNIZ deren endgültige Formel (in heutiger Schreibweise $\frac{n!}{n_1! n_2! \dots}$) auf der Seefahrt von England nach Holland im Oktober 1676 gefunden habe. Denn LEIBNIZ schrieb 1695 an JOH. BERNOULLI über sie: „Excogitavi olim mirabilem regulam“¹⁾; „mihi aliquando *naviganti* in mentem venit“²⁾ Jedenfalls notierte er sich schon am 12. November 1677, man könne $196\ 532$ ins Quadrat erheben, wenn man mit den einzelnen Summanden $2 + 30 + 500 + \dots$ nach einer Formel rechne. (Handschrift 9, Blatt 3, Rückseite.) Und im September 1678 finden sich die richtigen Formeln der ersten Potenzen ausgeschrieben.³⁾ Danach ist also CANTORS Grund dafür⁴⁾, daß LEIBNIZ die Polynomkoeffizienten erst nach 1691 ganz richtig habe berechnen können, nicht haltbar. LEIBNIZ hat auf diesem Gebiete ganz sicher die Priorität der ersten Entdeckung vor JAKOB BERNOULLI und DE MOIVRE, und zwar die Priorität um Jahrzehnte.

Nach diesen Ausführungen über die LEIBNIZschen Entdeckungen in andern Anwendungsgebieten der Kombinationslehre können wir uns nunmehr der Geschichte seiner zahlentheoretischen Studien zuwenden, die demselben Gedankenkreise entstammen und für deren Verständnis daher die vorangegangene Schilderung nötig war. Denn die Fortschritte, die LEIBNIZ in der Zahlentheorie gemacht hat, verdankt er fast ausschließlich kombinatorischen Hilfsmitteln.

Die Anregung zur Beschäftigung mit diesem durch VIÈTE, BACHET und besonders FERMAT wieder in Fluß gekommenen Gebiete empfing LEIBNIZ u. a. durch ARNAULD, der ihn 1675 auf die pythagoreischen Zahlen aufmerksam machte.⁵⁾ Er beschäftigte sich ferner mit dem Problem, ein rechtwinkliges Dreieck zu finden, dessen Flächeninhalt eine Quadratzahl ist, und zwar mit dem Beweise der Unmöglichkeit⁶⁾; er nannte dies das „problema FRÉNICLIANUM“, weil FRÉNICLE es veröffentlicht hatte; doch stammte es eigentlich von FERMAT, von dem FRÉNICLE vermutlich auch seinen Unmöglichkeitsbeweis übernommen hatte. LEIBNIZ arbeitete ferner an Aufgaben von folgender Art: Drei Zahlen zu finden, deren Summe ein Quadrat und deren Quadratsumme eine 4. Potenz ist⁷⁾; drei Zahlen zu finden, so daß die Summe und Differenz je zweier ein Quadrat ist⁸⁾; er versuchte diese und ähnliche diophantische Aufgaben zu lösen, indem er die Unbe-

1) LEIBNIZENS *Math. Schr.* III, 175. 2) LEIBNIZENS *Math. Schr.* III, 192.

3) *Math.* Vol. III 3, Blatt 8. Vgl. ferner III 4, Blatt 32. III 3, Scheda VII (Juni 1682). XII 1, Blatt 163. LEIBNIZENS *Math. Schr.* VII, 174—179 (*Nova algebrae promotio*).

4) CANTOR, *Vorl.* III², 45, 330.

5) *Math.* III B 8, Blatt 1, 2 (12. Dez. 1675). Vgl. ferner *Math.* III B 20 (4. Dez. 1678).

6) *Math.* IV 15 (29. Dez. 1678), gedruckt in LEIBNIZENS *Math. Schr.* VII, 120. IV 4 (Juli 1679), z. T. gedruckt bei COUTURAT, *Opusc.* 578.

7) *Math.* IV 4. III 16, 30. 8) *Math.* III B 19 (1. April 1676) III 16, 30.

kannten mit Hilfe seines dyadischen Zahlensystems besonders einfach schrieb.¹⁾

Am meisten aber interessierten ihn das ungelöste Rätsel der Anordnung der Primzahlen und die Untersuchungen über die Teilbarkeit der zusammengesetzten Zahlen. Auf diesem Gebiete verfolgte LEIBNIZ einen zuerst von PASCAL eingeschlagenen Weg weiter, der eine Verbindung der Kombinatorik und Zahlentheorie herstellte. Eine Kombinationszahl oder, was dasselbe ist, eine figurierte Zahl muß ihrem Wesen nach ganz sein. Da sie nun aber in der Formel die Form eines Bruches hat, so muß der Zähler durch den Nenner teilbar sein. So ergibt sich der Satz: Das Produkt von k aufeinander folgenden Zahlen ist teilbar durch das Produkt der k ersten Zahlen, $1 \cdot 2 \cdot 3 \dots k$, das wir jetzt gewöhnlich mit $k!$ bezeichnen.²⁾ Hieraus leitete er im Januar 1676 neue interessante Ergebnisse ab. $(y + 1)(y + 2)(y + 3)$ ist durch $1 \cdot 2 \cdot 3$ teilbar, oder $y^3 + 6y^2 + 11y + 6$ ist durch 6 teilbar. Schreibt man nun $12y - y$ statt $11y$, so folgt, daß auch $y^3 - y$ durch 6, also erst recht durch den Exponenten 3 teilbar ist und daß $\frac{y^3 - y}{y}$ oder $y^2 - 1$ ebenfalls durch 3 teilbar ist, falls nicht y selbst ein Vielfaches von 3 ist. Ein ähnlich einfacher Satz läßt sich bei der 4. Potenz nicht ableiten, während für die 2. Potenz selbstverständlich sowohl $y^2 + y$ wie $y^2 - y$ durch den Exponenten 2 teilbar ist. So weit war LEIBNIZ am 23. Januar 1676 in Handschrift 1 gekommen, in deren Überschrift er deshalb die Worte mit aufnahm: „des diviseurs des puissances“.

Weiter gelangte er noch im selben Monat in der zweiten Handschrift Der Herzog von ROANNEZ, PASCALS Freund, hatte LEIBNIZ von den Anfängen der Wahrscheinlichkeitsrechnung durch den Chevalier de MÉRÉ, PASCAL, FERMAT und HUYGENS berichtet und ihm die Aufgabe gestellt, die Zahl der möglichen Fälle beim Würfelspiel zu berechnen. LEIBNIZ verwandte dazu, ähnlich wie TARTAGLIA³⁾, die Formel für die Kombinationen und das PASCALsche Dreieck in der Anordnung, die wir oben kennen gelernt haben. Bei dieser Gelegenheit ließ er sich durch sein Interesse für das Problem der Teilbarkeit der Zahlen zu einer Abschweifung verführen, deren interessante Ergebnisse er an den Rand des begonnenen Entwurfes und auch quer über diesen weg schrieb. Die wichtigsten sehen in der GAUSSischen Bezeichnungsweise folgendermaßen aus:

1) Math. III 16, 29, 30 Vgl. COUTURAT, *Opusc.* 571.

2) Diesen Satz hatte schon PASCAL ausgesprochen und auf die gleiche Art bewiesen (*De numericis ordinibus tractatus*, prop. 5). Bei LEIBNIZ findet er sich zuerst, soviel ich sehe, in Handschr. 1 (3. Jan. 1676). Dann ist er auch übergegangen in die Handschr. 20, gedruckt in *LEIBNIZens Math. Schr.* VII 109—113.

3) *General trattato di numeri, et misure* II (1556), Bl. 17^r.

Der Zähler der y^{ten} Dreieckszahl:

$$(y+1)y = y^2 + y = y^2 + 2y - y = y^2 - y \equiv 0 \pmod{2}.$$

Die Zähler der y^{ten} Pyramidalzahl:

$$(y+2)(y+1)y = y^3 + 3y^2 + 2y = y^3 + 3y^2 + 3y - y = y^3 - y \equiv 0 \pmod{3}.$$

Ebenso:

$$(y+4)(y+3)(y+2)(y+1)y = y^5 + 10y^4 + 35y^3 + 50y^2 + 24y = y^5 - y \equiv 0 \pmod{5}.$$

So weit gelangt, fährt LEIBNIZ fort: „Habemus ergo theorema perelegans: potestatem quinti gradus latere minutam esse qvinarium. Unde crediderim, si continuetur, hanc progressionem prodituram $y^1 - y$ (id est 0) unitarius, $y^3 - y$ ternarius, $y^5 - y$ qvinarius, $y^7 - y$ septenarius.“ Er wollte also durch Induktion folgern, daß für jede ungerade Zahl n und für jede ganze Zahl y die Kongruenz gültig sei: $y^n - y \equiv 0 \pmod{n}$. Er überzeugte sich durch Zahlenrechnung davon, ob dies für $y = 2$ der Fall sei. Dabei stellte sich heraus, daß $2^9 - 2$ nicht durch 9 teilbar ist. LEIBNIZ schrieb daraufhin zur Reihe „ $2^9 - 2$ novenarius“ die Worte hinzu „non tamen rursus“ und fügte die Schlußbemerkung bei: „Ubi mirum solum novenarium dissentire, exemplum elegans inductionis deceptricis.“ Hätte er die Rechnung noch etwas weiter fortgesetzt, so würde er sicher durch Induktion gefunden haben, daß der Satz nicht für alle ungeraden Zahlen, sondern für alle Primzahlen gültig ist, und er hätte damit den FERMATSchen Satz durch eine nicht täuschende Induktion gefunden.

LEIBNIZ würde sogar auf dem angegebenen Wege einen vollständigen Beweis des FERMATSchen Satzes haben finden können. Denn der von ihm betrachtete Ausdruck ist derselbe, den später LAGRANGE¹⁾ benutzt hat, um gleichzeitig den FERMATSchen und den WILSONSchen Satz zu beweisen. Nach LAGRANGE ist nämlich

$$y^{p-1} - 1 \equiv (y + p - 1)(y + p - 2) \dots (y + 1) \pmod{p},$$

wenn p eine Primzahl ist. Daraus folgt, daß die Kongruenz $y^{p-1} \equiv 1 \pmod{p}$ $p - 1$ Wurzeln hat, nämlich: 1, 2, ..., $(p - 1)$, also alle zu p primen Zahlen y . Ferner folgt, da die LAGRANGESche Kongruenz für alle y gilt, daß die Koeffizienten der einzelnen Potenzen von y auf der linken und rechten Seite kongruent sind.

Also ist:

$$1 \cdot 2 \cdot 3 \dots (p - 1) \equiv -1 \pmod{p} \quad (\text{WILSONScher Satz}),$$

$$\sum_1^{p-1} 1 \cdot 2 \dots (p - 2) \equiv \sum_1^{p-1} 1 \cdot 2 \dots (p - 3) \dots \equiv \sum_1^{p-1} 1 \cdot 2 \equiv \sum_1^{p-1} 1 \equiv 0 \pmod{p}.$$

1) Nouvelles mémoires de l'académie de Berlin, Année 1771, p. 125.

So allerdings hätte LEIBNIZ noch nicht schließen können, da diese Schlußweise eine ausgebildete Methode des Rechnens mit Kongruenzen voraussetzt. Aber er hätte umgekehrt vorgehen können. Er wußte, daß

$$y^{n-1} + y^{n-2} \sum_1^{n-1} 1 + y^{n-3} \sum_1^{n-1} 1 \cdot 2 + \dots + 1 \cdot 2 \dots (n-1) \equiv 0 \pmod{n}$$

für alle ganzen Zahlen y und n ist. Ferner verstand er, wie wir gesehen haben, die symmetrischen Funktionen Σa^m durch die elementaren, $\Sigma abc \dots$ auszudrücken, also hätte er auch umgekehrt $\Sigma 1 \cdot 2 \cdot 3 \dots$ durch $\Sigma 1^m$ ausdrücken können. Wenn er also noch PASCALS Formeln für die Summen der Potenzen der aufeinander folgenden ersten ganzen Zahlen benutzt hätte, so würde er Regeln für die Teilbarkeit der Koeffizienten jener Kongruenz haben finden können. Führt man den skizzierten Weg wirklich aus, so ergibt sich, daß $\sum_1^{n-1} 1 \cdot 2 \cdot 3 \dots m$ durch n teilbar ist, solange n mit keiner der Zahlen $1, 2, 3, \dots, (m+1)$ einen gemeinsamen Teiler hat. Wenn also p eine Primzahl ist, so ist

$$\sum_1^{p-1} 1 \equiv \sum_1^{p-1} 1 \cdot 2 \equiv \dots \sum_1^{p-1} 1 \cdot 2 \dots (p-2) \equiv 0 \pmod{p}.$$

Daher ist auch $y^{p-1} + 1 \cdot 2 \cdot 3 \dots (p-1) \equiv 0 \pmod{p}$. Sonach ist der FERMATSche auf den WILSONSchen Satz zurückgeführt (oder umgekehrt). Nachdem LEIBNIZ den WILSONSchen Satz entdeckt hatte¹⁾, bestand also für ihn die Möglichkeit, mit seiner Hilfe auch den FERMATSchen Satz aus den Formeln der figurierten Zahlen abzuleiten.

1) LEIBNIZ hat in der Tat, wie VACCA im Boll. di bibl. e storia mat. 1899, festgestellt hat, den WILSONSchen Satz schon etwa ein Jahrhundert eher erkannt, als WARING ihn in seinen *Meditationes algebraicae* (Cantabrigiae 1770) veröffentlicht und LAGRANGE an der angegebenen Stelle ihn zuerst bewiesen hat. LEIBNIZ hat nämlich in Handschrift 25 die Reste von $1!, 2!, 3! \dots 16! \pmod{2}$, ferner die Reihe $\pmod{3} \pmod{4} \dots \pmod{13}$ zusammengestellt und daraus geschlossen: „Productus continuorum usque ad numerum, qui anteprecedit datum, divisus per datum relinquit 1, si datus sit primitivus. Sin datus sit derivativus, relinquet numerum, qui cum dato habeat communem mensuram unitate majorem.“ D. h. $p-2! \equiv 1 \pmod{p}$, wenn p eine Primzahl ist, dagegen $n-2! \equiv m \pmod{n}$, wobei m einen gemeinsamen Faktor mit n besitzt. Würde man die erste Kongruenz mit $p-1$ multiplizieren, so würde sich ergeben: $p-1! \equiv p-1 \equiv -1 \pmod{p}$, d. h. es würde der bekannte WILSONSche Satz folgen. LEIBNIZ hat nun seinen induktiv gefundenen Satz noch bei der nächsten Primzahl, $p=17$, nachgeprüft, sich dabei aber verrechnet. Er gibt nämlich an: $11! \equiv 16 \dots 15! \equiv 16, 16! \equiv 1 \pmod{17}$, während in Wirklichkeit $11! \equiv 1 \dots 15! \equiv 1, 16! \equiv 16$ ist. Durch diesen Rechenfehler ist er veranlaßt worden, seinen richtigen Satz abzuändern und noch den falschen Zusatz zu machen: $\dots \text{relinquit } \{1 \text{ vel complementum ad } 1\}$, d. h. $p-1$. In der Tat ist ja bei seiner Rechnung $15! \equiv 17-1$, während in Wirklichkeit $15! \equiv 1$ ist. So erklärt sich dieser falsche Zusatz, der VACCA unverständlich war.

Aber LEIBNIZ ist diesen Weg nicht gegangen, sondern hat den Satz später auf eine viel einfachere Weise gewonnen. Er hat überhaupt den Gedankengang, der ihn eigentlich schon 1676 auf den FERMATSchen Satz, wenigstens induktiv, hätte führen müssen, nicht weiter in dieser Richtung fortgesetzt, sondern ist nach einer anderen Seite abgebogen und hat die gewonnenen Ergebnisse folgendermaßen ausgesprochen: „Omnis quadratus est aut ternarius aut unitate major ternario, omnis quadrato-quadratus aut quaternarius aut unitate major quinario.“ Ferner folgert er aus $y^5 - y \equiv 0 \pmod{5}$ und dem Satze, nach dem die Differenz zweier verschiedenen Potenzen einer Zahl immer eine gerade Zahl sein muß, daß $y^5 - y$ durch 10 teilbar ist, daß also im dekadischen Zahlensystem y^5 und y am Schlusse dieselben Ziffern haben. Ebenso haben y^6 und y^2 , y^7 und y^3 usw. dieselben Ziffern am Schluß:

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
1	2	4	8	16	32	64	128	236

„Si exacte inspicias, est quidam periodus in numeris progressionis geometricae, qui semper ordine redit. . . . Scilicet semper aequidistantes a se invicem subtracti relinquent denarios.“ (Handschrift 2.) Hieraus ergibt sich ein sehr enger Zusammenhang zwischen dem FERMATSchen Satze und der Theorie der Potenzreste sowie der periodischen Dual- und Dezimalbrüche. Die nähere Verfolgung dieses Zusammenhanges ist es denn auch gewesen, die LEIBNIZ in den nächsten Jahren zur wirklichen Neuentdeckung des FERMATSchen Satzes geführt hat.

Über die gewonnenen Ergebnisse hat LEIBNIZ sich nach Handschrift 4 am 10. Februar 1676 mit dem Physiker MARIOTTE unterhalten und dabei gehört, daß FRÉNICLE derartige Sätze auf andere Art beweisen könne; doch scheint MARIOTTE nicht näher darüber unterrichtet gewesen zu sein. — Die von LEIBNIZ gefundenen Sätze finden sich auch in der 3. und 5. Handschrift. Die letztere, der von GERHARDT gedruckte „Conspectus calculi“, muß auch aus dieser Zeit stammen, weil in ihm¹⁾ die ganz speziellen Sätze über die 3. und 5. Potenz schon als „consequentiae elegantes“ bezeichnet werden. Auch das macht diese Datierung gewiß, daß LEIBNIZ hier noch keinen andern Weg kennt, um den Primzahlcharakter einer Zahl festzustellen, als die Zerlegung in Faktoren²⁾

In den nächsten Jahren dagegen fand er durch eifrige Beschäftigung mit den Primzahlen neue Mittel, um ohne Faktorenzerlegung über Teilbarkeit oder Unteilbarkeit einer gegebenen Zahl zu entscheiden. Der Gewinn solcher Mittel war für die Zahlentheorie von größter Wichtigkeit. Denn bis dahin gab es keinen andern Weg, um den Primzahlcharakter einer be-

1) LEIBNIZens Math. Schr. VII, 100.

2) LEIBNIZens Math. Schr. VII, 93.

stimmten, vorgelegten Zahl p zu erkennen, als ihre Teilbarkeit durch die sämtlichen Primzahlen $\leq \sqrt{p}$ der Reihe nach durchzuprobieren, was bei größeren Zahlen bald praktisch unmöglich wird. Es war also ein sehr richtiger Gedanke von LEIBNIZ, wenn er hier nach Erleichterungen spürte. Tatsächlich ist es ihm auch gelungen, brauchbare Methoden auszubilden, um ziemlich leicht festzustellen, daß eine bestimmte Zahl keine Primzahl sein kann. Das Problem der positiven Erkennung einer Primzahl glaubte er später mit Hilfe des FERMATSchen Satzes auch lösen zu können, freilich mit Unrecht. Hier haben erst EULER und LAMBERT ein Jahrhundert später den richtigen Weg gefunden.

Die erste Tatsache, die LEIBNIZ auf diesem Gebiete fand, war die, daß jede Primzahl, die größer als 3 ist, um eins größer oder kleiner als ein Vielfaches von 6 sein muß.¹⁾ LEIBNIZ hat diesen Satz im wesentlichen Anfang April aus der folgenden Anordnung der zusammengesetzten Zahlen erschlossen (Handschrift 6):

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
Binarii:	•			•			•			•			•			•			•			•			•	
Ternarii:	•			•			•			•			•			•			•			•			•	
Qvaternarii:	•				•					•			•				•				•				•	

In Worte gefaßt hat er die Regel zuerst am 7. September 1677 in Handschrift 8. Die Entdeckung schien ihm damals sehr wichtig, und er fügte daher eine genaue Bemerkung über die Abfassungszeit hinzu mit der Begründung: „ut appareat, qvo progressu paulatim in hoc arcanum numericum penetraverim.“ Aber er war sich doch klar darüber, daß er hier wohl ein notwendiges, aber kein hinreichendes Kennzeichen der Primzahlen gefunden habe, und erklärte es in derselben Handschrift 8 für eine „qvaestio ingeniosissima“ festzustellen, wie viel man gegen 1 wetten könne, daß eine Zahl, die nach 6 den Rest 1 oder 5 lasse, wirklich eine Primzahl sei. Immerhin hielt er seine Entdeckung auch so schon einer Mitteilung im Journal des savants für würdig: *Observation nouvelle de la manière d'essayer, si un nombre est primitif*, Februar 1678.²⁾

LEIBNIZ suchte weiter nach einem notwendigen und hinreichenden Primzahlkriterium. Offenbar ist eine Zahl p stets dann und nur dann eine Primzahl, wenn sie zum Produkte der Primzahlen $2 \cdot 3 \cdot 5 \cdots q$ (wobei q die größte Primzahl bedeutet, die $\leq \sqrt{p}$ ist) prim ist (Handschrift 7,

1) Denselben Satz hat nach VACCA (Bibl. math. 2, 1901, p. 149) schon PIETRO BONGO in seinem Werke *Numerorum mysteria* (1599) ausgesprochen.

2) LEIBNIZens Math. Schr. VII, 119, 120.

Blatt 2, Vorderseite). Diesen bekannten Satz, der aber wegen der Größe des Produktes zur wirklichen Feststellung einer Zahl als Primzahl meist gänzlich ungeeignet ist, suchte LEIBNIZ so umzugestalten, daß er für die Rechnung brauchbar würde. Er glaubte schon mit dem viel kleineren Produkte $2 \cdot 3 \cdot 5 \cdots r$ auszukommen, das gerade noch $< p$ ist. Im Dezember 1677 notierte er sich darüber folgende Regel (Handschrift 10): Wenn man das Produkt der aufeinander folgenden Primzahlen 2, 3, 5... um 1 vermehrt oder vermindert, so erhält man eine neue Primzahl, wenn man es dagegen um einen der anderen Faktoren vermehrt oder vermindert, so erhält man eine zusammengesetzte Zahl. Der zweite Teil der Regel ist selbstverständlich richtig. Dagegen braucht weder eine Primzahl immer die Form $2 \cdot 3 \cdot 5 \cdots p \pm 1$ zu haben, noch ist eine Zahl von der Form $2 \cdot 3 \cdot 5 \cdots p \pm 1$ immer eine Primzahl. Denn erstens ist 11 weder gleich $2 \cdot 3 + 1$, noch gleich $2 \cdot 3 \cdot 5 - 1$, und zweitens ist $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ und $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$. Vielmehr läßt sich, wie schon EUKLID wußte und zum Beweis der unendlichen Anzahl der Primzahlen benutzte, nur behaupten, daß $2 \cdot 3 \cdots p \pm 1$ entweder selbst eine Primzahl ist oder Primzahlen als Faktoren enthält, die unter den Primzahlen 2, 3, ..., p noch nicht vorgekommen sind.

Auch mit dieser neuen Regel hatte also LEIBNIZ sein Ziel einer allgemeinen Primzahlgleichung noch nicht erreicht. Er suchte deshalb weiter und fand endlich das Gesuchte von ganz anderen Seiten her, als nämlich die Theorie der Dual- und Dezimalbrüche, die Potenzsummenformeln und der polynomische Lehrsatz ihn nacheinander auf den FERMATSchen Satz führten.

Mit den Perioden der Dual- und Dezimalbrüche beschäftigte sich LEIBNIZ vom Jahre 1677 an. Zur gleichen Zeit schrieb auch WALLIS in seiner *Algebra*¹⁾ darüber. Dieser war der Meinung, der erste zu sein: „Nescio an quisquam me prior eam distincte examinaverit.“²⁾ Doch war LEIBNIZ schon viel weiter gelangt als WALLIS. LEIBNIZ wußte nämlich nicht nur wie jener, daß die Perioden der Dezimalbruchentwicklung von $\frac{1}{n}$ höchstens $n - 1$ Stellen und häufig einen echten Teiler von $n - 1$ als Stellenzahl haben, sondern genauer, daß das letztere immer dann eintritt, wenn n eine Primzahl ist. Außerdem aber hatte er schon die wichtigste Tatsache des ganzen Gebietes erkannt, nämlich seine enge Verbindung mit dem FERMATSchen Satze, die erst fast ein Jahrhundert später von LAMBERT wieder entdeckt worden ist.³⁾

1) Handschriftlich fertiggestellt 1676, zuerst gedruckt: englisch 1685, dann lateinisch in seinen *Opera omnia*, Oxoniae 1693. 2) *Opera* II, 364

3) *Acta Helvetica* 1758. (*Nova acta eruditorum* 1769, p. 107—128: *Adnotatio quaedam de numeris eorumque anatomia*. Vgl. TROPFKE, *Gesch.* I, 94, 95.

LEIBNIZ wurde auf die Perioden der Dual- und Dezimalbrüche durch seine Beschäftigung mit den dyadischen Zahlen und den Potenzresten geführt. Einen speziellen Fall des grundlegenden Satzes hatte er, wie erwähnt, schon 1676 gefunden: Die steigenden Potenzen von 2 lassen nach 10 immer die Reste 2, 4, 8, 6 in periodischer Folge. Wenn man also $\frac{1}{10}$ in einen Dualbruch entwickelt, so erhält man, nachdem diese Reste alle vorgekommen sind, wieder dieselben Reste, demnach auch dieselben Quotienten, mit anderen Worten eine Periode von 4 Stellen. Ebenso lassen die Potenzen von 2 nach jeder anderen Zahl n , die nicht selbst eine Potenz von 2 ist, eine periodisch wiederkehrende Reihe von Resten, und deshalb ergibt auch $\frac{1}{n}$ einen periodischen Dualbruch. Z. B. ist $\frac{1}{3}$, dyadisch geschrieben

$$\frac{1}{11} = 0,01\,01\,01\,\dots$$

Nun können aber offenbar bei der Division durch n höchstens $n - 1$ verschiedene Reste auftreten, also kann die Periode höchstens $n - 1$ Stellen haben. LEIBNIZ glaubt aber noch mehr daraus schließen zu können. Da nämlich der Dividendus 1 sich als der erste Rest betrachten läßt, so meint er, auch die 2. Periode beginne damit, daß der Rest 1 wieder auftrete. Demnach würde es immer eine Potenz von 2 mit dem Exponenten $k < n$ geben, die, durch n geteilt, den Rest 1 läßt: $2^k \equiv 1 \pmod{n}$, wobei $k < n$ ist.

In solcher Allgemeinheit ist diese Ausdehnung des FERMATSchen Satzes auf zusammengesetzte Moduln allerdings falsch. LEIBNIZ hat den Irrtum aber später selbst berichtigt. Nur dann nämlich beginnt die 2. Periode beim Reste 1, wenn n nicht durch 2 teilbar ist. Ist n dagegen eine gerade Zahl, so beginnt die Periode mit einem späteren Reste, z. B. in dem oben erwähnten Falle, $n = 10$, mit dem 2. Reste. Vor der 4ziffrigen Periode kommen dann noch Vorziffern. Demnach ergeben die Brüche mit geradem Nenner nichtreinperiodische Dualbrüche („non pure periodicos“, Handschrift 38), alle Brüche mit ungeradem Nenner dagegen lassen sich in reinperiodische Dualbrüche entwickeln.

Ähnliches gilt im triadischen, tetradischen . . . dekadischen System. Im triadischen System allerdings kann der erste Rest außer 1 auch 2 sein (nämlich bei $\frac{2}{n}$), im tetradischen 1, 2, 3 und im dekadischen 1, 2 . . . 9. Durch diesen Gedankengang scheint LEIBNIZ auf den Satz geführt worden zu sein: „Omnis numerus exacte dividit aliquem numerum progressionis geometricae duplae unitate minutum. Omnis numerus exacte dividit aliquem numerum progressionis geometricae triplae vel unitate vel binario minutum etc.“ (Handschr. 12). Nämlich wenn die geometrische Reihe, deren Quotient 3 ist, das 1. Glied 1 hat, so läßt ein Glied der geometrischen Reihe bei der Division durch n (vorausgesetzt allerdings, daß n und 3 teilerfremd

sind, was LEIBNIZ in dieser ersten Zeit übersehen und erst später verbessert hat) den Rest 1, und zwar ist dies spätestens das Glied der Form $3^n - 1$. Ist dagegen das erste Glied gleich 2, so läßt dasselbe spätere Glied den Rest 2.

Die Dezimalbrüche stehen in der gleichen Beziehung zu den Potenzen von 10 wie die Dualbrüche zu den Potenzen von 2. So ergibt sich denn, daß jede Zahl n (die zu 10 prim ist, was LEIBNIZ wieder zunächst vergessen hat) in irgendeiner um eins verminderten Potenz von 10, also in irgendeiner Zahl der Form 999 ... aufgeht, und zwar spätestens in der Zahl mit $n - 1$ Neunenn, oder anders ausgedrückt, daß $\frac{1}{n}$ als Dezimalbruch eine Periode von höchstens $n - 1$ Stellen ergibt.¹⁾ Jeder Bruch $\frac{1}{n}$, dessen Nenner zu 10 prim ist, läßt sich also durch einen reinperiodischen Dezimalbruch mit einer endlichen Anzahl von Periodenstellen darstellen.

Diesen wichtigen Satz versuchte LEIBNIZ, wie nebenbei bemerkt sein mag, schon 1677 zu einem Beweise für die Irrationalität von π zu benutzen. Seit 1674 kannte er, wie erwähnt, die Formel

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \dots$$

Entwickelt man nun sämtliche Brüche in Dezimalbrüche, so erhält man immer länger werdende Perioden. Die Summe aller, meint LEIBNIZ, hat demnach eine unendlich lange Periode, ist also irrational. Der Beweis ist unrichtig. Denn eine Summe von unendlich vielen, immer länger werdenden periodischen Dezimalbrüchen kann sehr wohl rational sein. Z. B. ist

$$1 + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} \dots = \frac{1}{1 - \frac{1}{3}} = \frac{3}{2}.$$

Aber interessant ist doch, daß LEIBNIZ schon damals wenigstens einen Beweis der Irrationalität zu geben versuchte und die Hoffnung aussprach, daß es auf ähnliche Weise auch gelingen würde, die Unmöglichkeit der Quadratur des Kreises mit Zirkel und Lineal zu zeigen.²⁾ Wirklich gelungen ist bekanntlich der Beweis, und zwar zunächst nur der der Irrationalität von π , erst LAMBERT³⁾ im Jahre 1766, und zwar mit Hilfe der Kettenbruchentwicklung, statt der von LEIBNIZ benutzten Dezimalbruchentwicklung.

1) Umgekehrt, um die Zahl der Periodenstellen von $\frac{1}{n}$ genauer festzustellen, muß man zusehen, in welcher der Zahlen 9, 99, 999 ... n zuerst aufgeht. Diese Regel gibt LEIBNIZ in Handschr. 38 und 39.

2) „Ex eo ... aliqua videtur aperiri via ad demonstrandam quadraturarum quadrandarum impossibilitatem. Certe illud hinc jam consecutus sum, ut possim demonstrare diametrum et circumferentiam non esse inter se in ratione numeri ad numerum, quod hactenus fecit nemo.“ (Handschr. 9.)

3) *Beyträge zum Gebrauche der Mathematik* II, Berlin 1770, S. 140—169, nach der Vorrede schon 1766 geschrieben. Vgl. TROFFKE, *Gesch.* II, 133.

Seine Entdeckungen über die Perioden der Dezimalbrüche hat LEIBNIZ später noch weiter verfolgt und verbessert, besonders seitdem er den FERMATschen Satz genauer kennen gelernt hatte. Hierher gehören außer den erwähnten Handschriften 9 und 12 noch die Handschriften 11 und 14 und vor allem eine aus dem Januar 1687 stammende ausführliche Abhandlung, Handschrift 38 und 39, über die er selbst geschrieben hat: „*insignia inventa*“ und die mit den Worten schließt: „*cuius rei (nämlich der Anzahl der Periodenstellen bei Primzahlennenner) regula et progressionem detecta, puto arcanam primitivorum numerorum naturam magis tandem detectum iri*“. Die historische Entwicklung ist anders verlaufen: nicht die Lehre von den periodischen Dezimalbrüchen hat die Zahlentheorie gefördert, sondern umgekehrt, der systematische Ausbau der Zahlentheorie durch GAUSS hat die Lehre von den periodischen Dezimalbrüchen zur Vollendung geführt. Ich breche deshalb hier mit der Erörterung der LEIBNIZschen Untersuchungen über die Perioden der Dezimalbrüche ab, um mich der rein zahlentheoretischen Formulierung des FERMATschen Satzes zuzuwenden.

LEIBNIZ hatte zunächst, wie wir sahen, fälschlich gemeint, für jede beliebige Zahl n ließe sich ein $k < n$ finden, so daß $2^k \equiv 1 \pmod{n}$, ebenso $3^k \equiv 1 \pmod{3}$, allgemein $a^k \equiv 1 \pmod{n}$ würde. Er bemerkte aber bald, daß der Satz in dieser Allgemeinheit unrichtig sei. Ist dagegen n eine Primzahl, so gilt er sicher für alle a , die nicht gerade Vielfache von n sind. Aus diesem Grunde sah sich LEIBNIZ genötigt, nachträglich in den Handschriften 12 und 14 zu dem Satze: „*Omnis numerus exacte dividit aliquem numerum progressionis geometricae duplae unitate minutum*“ die Notiz hinzuzufügen: „*{falsum nisi de primitivo}*“, die sich durch Schrift und Tinte als später hinzugefügt zu erkennen gibt.

Ist aber n eine Primzahl, so kann man den Satz auch noch genauer formulieren. Denn in diesem Falle erfüllt sicher $k = n - 1$ die verlangte Bedingung, und es ist $a^{n-1} \equiv 1 \pmod{n}$. Diese Tatsache hat LEIBNIZ am 12. September 1680 zugleich mit ihrem Beweise entdeckt (Handschr. 13). Von diesem Tage stammt sonach der erste bekannte Beweis des FERMATschen Satzes. Da LEIBNIZ meinte, auch umgekehrt behaupten zu können, daß jener Satz nur für Primzahlen gültig sei, so war damit endlich — so glaubte er — das lange gesuchte notwendige und hinreichende Kennzeichen der Primzahlen gefunden, das er noch am 18/28. Mai 1680 in einem Briefe an CLÜVER vermißt hatte.¹⁾

LEIBNIZ fand den Satz oder vielmehr einen allgemeinen Satz, der den FERMATschen einschließt, bei Gelegenheit seiner Untersuchung der „Formen“,

1) *LEIBNIZens Math. Schr.* VII, 18. *Resolutio numerorum in factores primitivos et inventio certae notae reciprocae, qua primitivi a derivativis sine tabulis et calculi molestia discerni possint, res est nondum satis a quoquam tractata.*

insbesondere bei der Zurückführung der Potenzsummen auf die elementaren symmetrischen Funktionen. LEIBNIZ hatte am 12. September einen Entwurf begonnen, der die Überschrift trug: „Formarum reductio ad simplices“ (Handschr. 13). Hier stellte er zunächst die jetzt sogenannten NEWTONSchen Potenzsummenformeln zusammen, die er, wie erwähnt, seit spätestens 1678 kannte. Bei der Formel für die 5. Potenz angekommen, fiel ihm plötzlich auf, daß sämtliche Koeffizienten außer dem ersten $= 5$ seien, ebenso bei a^2 alle $= 2$ und bei a^3 alle $= 3$, dagegen bei a^4 nicht alle $= 4$. Da er jetzt mehr als 1676 an die Beschäftigung mit Primzahlen gewöhnt war, schloß er sofort induktiv (was er damals bei ähnlicher Gelegenheit versäumt hatte): Die Teilbarkeit durch den Exponenten wird bei allen Primzahlen vorhanden sein. Also folgt

$$(a + b + c + \dots)^p - a^p - b^p - c^p - \dots \equiv 0 \pmod{p},$$

wenn p eine Primzahl ist. Setzt man insbesondere $a = b = c \dots = 1$ und $a + b + c + \dots = 1 + 1 + 1 + \dots = x$, so ergibt sich

$$x^p - x \equiv 0 \pmod{p}.$$

Ist $x = 2$ und p eine Primzahl > 2 , so folgt daraus $2^{p-1} - 1 \equiv 0 \pmod{p}$.

LEIBNIZ erinnert sich sofort daran, daß er einen ähnlichen Satz von den Dualbrüchen her schon kennt. Jede Zahl n teilt ja, wie er meint, irgendein um 1 vermindertes Glied der geometrischen Reihe mit dem Quotienten 2. Als neu gewonnen ist also die Erkenntnis hinzuzufügen, daß dies für die Primzahlen n immer gerade das Glied 2^{n-1} ist. LEIBNIZ vermutet, daß dieser Satz auch umkehrbar sein wird: Wenn nicht das $(n-1)^{\text{te}}$, sondern schon ein früheres Glied die Teilbarkeitseigenschaft hat, so ist n keine Primzahl. „Videtur haec esse proprietas reciproca numeri primitivi“ (Handschrift 13).

Die letzte Vermutung ist unrichtig, insofern sie sich auf die spezielle geometrische Reihe mit dem Quotienten 2 bezieht. Denn erstens kann auch bei Teilung durch eine Primzahl schon ein früheres Glied, 2^k , den Rest 1 lassen, wenn nur k ein Teiler von $n-1$ ist, und zweitens gibt es auch Nichtprimzahlen, nach denen das $(n-1)^{\text{te}}$ Glied den Rest 1 läßt, wie ich gleich noch näher ausführen werde.

LEIBNIZ hat selbst gefühlt, daß nicht nur für seine Umkehrung der Beweis noch fehlt, sondern auch der Beweis des direkten Satzes unvollständig ist. Denn daß die Koeffizienten, die in den Potenzsummenformeln auftreten, immer alle durch n teilbar sind, wenn n eine Primzahl ist, das hat er nur induktiv, und zwar nur für wenige Fälle gezeigt. Diese Lücke hat er aber bald ausgefüllt, indem er noch einen weiteren Beweis fand, bei dem die Teilbarkeit der benutzten Koeffizienten leicht streng gezeigt werden kann. Vielleicht noch am 12. September 1680 oder wenige Tage später sah er näm-

lich, daß man den besonderen Fall $2^p - 2 \equiv 0 \pmod{p}$ auch aus dem binomischen Satze ableiten könne. Denn es ist ja

$$\begin{aligned}(1 + 1)^3 &= 1 + 3 + 3 + 1 \\(1 + 1)^4 &= 1 + 4 + 6 + 4 + 1 \\(1 + 1)^5 &= 1 + 5 + 10 + 10 + 5 + 1.\end{aligned}$$

Also ist $2^3 - 2$ durch 3, ebenso $2^5 - 2$ durch 5, aber nicht $2^4 - 2$ durch 4 teilbar.¹⁾ Daß aber die hier auftretenden Binomialkoeffizienten einer Primzahlpotenz außer dem ersten und letzten durch den Primzahlexponenten teilbar sind, das vermochte er 1681 leicht zu zeigen, als er aus deren Formeln, die ja zugleich Formeln der „numeri combinatorii“ sind, Regeln für die Teilbarkeit von Zahlen ableitete. Denn wenn p eine Primzahl ist, so kann in keinem der Brüche

$$\frac{p}{1}, \frac{p(p-1)}{1 \cdot 2}, \dots, \frac{p(p-1) \dots 1}{1 \cdot 2 \dots (p-1)}$$

der Faktor p des Zählers fortgehoben werden. (Handschrift 18.)

Mit den gleichen Hilfsmitteln versuchte LEIBNIZ nun auch seine Umkehrung zu beweisen, kam allerdings in Handschrift 18 noch nicht damit zustande, meinte aber in Handschrift 19²⁾ fälschlich, das Ziel erreicht zu haben. Er hielt den folgenden Beweis für ausreichend, wie dessen Aufnahme in die zusammenfassende Darstellung des ganzen Gebietes, Handschrift 34, zeigt:

Wenn n keine Primzahl, sondern etwa $= r \cdot s$ ist (wobei r den kleinsten in n enthaltenen Primzahlfaktor bedeutet), so sind die Zahlen $n - 1, n - 2 \dots, n - (r - 1)$ nicht durch r teilbar. Also kann sich in dem Koeffizienten des $(r + 1)$ ten Gliedes von $(1 + 1)^n$:

$$\frac{n(n-1) \dots (n-r+1)}{1 \cdot 2 \dots r}$$

1) Diesen Beweis hat LEIBNIZ mit flüchtiger Schrift und blasser Tinte ganz unten auf den (heute schon z. T. abgerissenen) Rand der Handschrift 13 geschrieben.

2) Die Handschrift III 26 enthält zwei Entwürfe der Abhandlung: De primitivis ex tabula combinatoria (Dez. 1681) und den Entwurf der damit zusammenhängenden Abhandlung: De primitivis et divisoribus ex tabula combinatoria, der in *LEIBNIZENS Math. Schr.* VII 109—113 gedruckt ist. Die ersten Entwürfe geben den Beweis der Umkehrung des FERMATSchen Satzes aus den Kombinationszahlen, dienen also der Aufgabe der Primzahlerkennung. Der dritte Entwurf dagegen beschäftigt sich nur mit der Ableitung von Teilbarkeitsregeln aus den Kombinationszahlen, so daß der erste Teil des Titels eigentlich auf ihn nicht recht mehr paßt. Es ist merkwürdig, daß GERHARDT die beiden ersten, mindestens ebenso interessanten Entwürfe gar nicht beim Druck berücksichtigt und nicht einmal das Datum, das offenbar für den dritten Entwurf auch ungefähr richtig ist, angegeben hat. So sieht sich CANTOR (*Vorl.* III², 44) zu einer bloßen Vermutung über die Abfassungszeit der bei GERHARDT gedruckten Abhandlung genötigt, die allerdings ziemlich genau das Richtige trifft (1680).

der Faktor r des Nenners nur gegen den ersten Faktor des Zählers fort-heben. Also ist dieser Koeffizient, der ja eine ganze Zahl sein muß, nicht mehr durch n , sondern nur noch durch s teilbar. In der Tat ist, da 4 den Faktor 2 enthält, der Koeffizient des $(2 + 1)^{\text{ten}}$ Gliedes von $(1 + 1)^4$, $\frac{4 \cdot 3}{1 \cdot 2}$ nicht mehr durch 4, sondern nur noch durch 2 teilbar. Es ist also bewiesen, daß nicht alle Glieder in der Entwicklung von $2^n - 2$, wenn n keine Primzahl ist, durch n teilbar sind. LEIBNIZ folgert daraus, daß auch $2^n - 2$ nicht durch n teilbar ist — mit Unrecht, denn es kann sehr wohl einmal, wenn auch nur in besonderen Fällen, die Summe durch n teilbar sein, wenn die Summanden nicht teilbar sind.

Aus den Formeln der Binomialkoeffizienten ist der FERMATSche Satz zunächst nur für die Basis 2 bewiesen. Um ihn in den übrigen Fällen abzuleiten, wendet LEIBNIZ nicht wie später EULER den Schluß von n auf $n + 1$ an, sondern beruft sich auf den polynomischen Lehrsatz, den er ja, wie erwähnt, schon 1676 entdeckt hatte. Wenn $x = a + b + c + \dots$ ist, so ist

$$x^n = a^n + f a^{n-1} b + g a^{n-2} b^2 + h a^{n-2} b c + \dots$$

Wenn n eine Primzahl ist, so sind sämtliche Polynomkoeffizienten f, g, h, \dots durch n teilbar, also ist auch $x^n - a^n$ durch n teilbar. Für $a = b = c = \dots = 1$ folgt daraus: $x^n - x = 0 \pmod{n}$, und wenn x und n prim sind: $x^{n-1} - 1 \equiv 0 \pmod{n}$. (So wohl zuerst in der leider nicht datierten Handschrift 30, dann in der *Nova algebrae promotio*.¹⁾)

Man könnte nun meinen, daß bei allgemeiner Basis der LEIBNIZsche Beweis der Umkehrung des FERMATSchen Satzes ausreichend sei, daß also die Kongruenz $x^{n-1} \equiv 1 \pmod{n}$ für alle zu n primen x nur dann erfüllt sein könne, wenn n eine Primzahl sei. Da nach einer brieflichen Mitteilung von Herrn Professor BACHMANN in Weimar über die Richtigkeit einer solchen Umkehrung noch nichts in der Literatur festgestellt ist, so habe ich zu ihrer Prüfung nach den Bedingungen gesucht, denen a und n genügen müssen (n als zusammengesetzte Zahl vorausgesetzt), wenn die FERMATSche Kongruenz für $x = a$ und den Modul n bestehen soll. Es sind die folgenden:

Es sei $n = p^\alpha q^\beta r^\gamma \dots$ die Darstellung von n durch die ganzzahligen Potenzen von lauter verschiedenen wachsenden Primzahlen $(2, 3, 5 \dots)$; ferner seien $k, l, m \dots$ die Exponenten, zu denen $a \pmod{p}, \pmod{q}, \pmod{r} \dots$ gehört, und $\kappa, \lambda, \mu \dots$ die größten Exponenten von $p, q, r \dots$, für die noch $a^k \equiv 1 \pmod{p^\kappa}, a^l \equiv 1 \pmod{q^\lambda}, a^m \equiv 1 \pmod{r^\mu} \dots$ ist. Bei diesen Festsetzungen ist für eine bestimmte zu $pqr \dots$ prime Zahl a stets dann und nur dann $a^{n-1} \equiv 1 \pmod{n}$, wenn $\alpha \leq \kappa, \beta \leq \lambda, \gamma \leq \mu \dots$ und k Teiler von $q^\beta r^\gamma \dots - 1$, l Teiler von $p^\alpha r^\gamma \dots - 1$, m Teiler von $p^\alpha q^\beta \dots - 1, \dots$ ist.

1) LEIBNIZens Math. Schr. VII, 180 und 181.

Daraus folgt: wenn n eine Potenz p^α einer Primzahl ist, so kann die FERMATSche Kongruenz wohl für bestimmte x bestehen (z. B. ist $8^3 \equiv 8^2 \equiv 1 \pmod{3^2}$, $3^{120} \equiv 3^{10} \equiv 1 \pmod{11^2} \dots$), aber nicht für alle zu n primen x . Denn für die primitiven Wurzeln $b \pmod{p^\alpha}$ ist der kleinste Exponent, bei dem $b^h \equiv 1 \pmod{p^\alpha}$ wird, $h = (p-1)p^{\alpha-1}$. Also kann nicht schon $b^k \equiv 1 \pmod{p^\alpha}$ sein, wo $k \leq p-1$ ist.¹⁾

Ebenso wenn n ein Produkt zweier Primzahlen $p \cdot q$ ist, so kann die FERMATSche Kongruenz für bestimmte x sehr wohl gelten (z. B. ist $4^{11} \equiv 4^2 \equiv 1 \pmod{3 \cdot 5}$, $3^{90} \equiv 3^6 \equiv 1 \pmod{7 \cdot 13}$, $2^{340} \equiv 2^{10} \equiv 1 \pmod{11 \cdot 31} \dots$), aber nicht für alle zu n primen x . Denn die eine Kongruenz, der die geeigneten x genügen müssen, ist $x^{p-1} \equiv 1 \pmod{q}$. Diese Primzahlkongruenz hat aber nur $p-1$ Wurzeln unter den Zahlen bis q , also $(p-1)p$ Lösungen bis pq , während es $(p-1)(q-1)$ zu n prime Zahlen gibt. Es gibt also sicher $(p-1)(q-p-1)$ prime Zahlen x , für die x^{n-1} nicht $\equiv 1 \pmod{n}$ ist. (Der Fall $p=2$, $q=3$, in dem $q-p-1=0$ werden würde, kann außer Betracht gelassen werden, da $a^{2p-1} \equiv a \pmod{2p}$ für alle zu $2p$ primen a ist, also nie $a^{n-1} \equiv 1 \pmod{n}$ werden kann, wenn $n=2p$ ist, außer für $a \equiv 1$.)

Wenn aber n ein Produkt von drei oder mehr verschiedenen Primzahlen ist, so steht dem Erfülltsein der Kongruenz $x^{n-1} \equiv 1 \pmod{n}$ für alle zu n primen x kein Hindernis entgegen²⁾, und ich habe tatsächlich Zahlen gefunden, für die die Möglichkeit wirklich wird, z. B.

$$n = 3 \cdot 11 \cdot 17; 5 \cdot 13 \cdot 17, 5 \cdot 17 \cdot 29, 5 \cdot 29 \cdot 73; 7 \cdot 13 \cdot 19, \dots$$

Die LEIBNIZSche Umkehrung des FERMATSchen Satzes ist also auch bei allgemeiner Basis falsch. Die richtige Umkehrung heißt vielmehr: Wenn für ein bestimmtes a die Kongruenz $a^h \equiv 1 \pmod{n}$ für $h = n-1$ erfüllt ist, dagegen niemals gilt, wenn h ein echter Teiler von $n-1$ ist, so ist n Primzahl. (Dieser von LUCAS stammende Satz³⁾ läßt sich übrigens aus dem obigen Satze aufs neue beweisen). Die LEIBNIZschen Bemühungen haben demnach nur insofern Wert, als sie zum erstenmal auf die Notwendigkeit einer Umkehrung des FERMATSchen Satzes hingewiesen haben, um daraus ein Mittel abzuleiten, die Primzahlen ohne Durchprobieren der

1) Während des Druckes hat die genauere Untersuchung mich auf den Beweis des folgenden Satzes geführt: Die Kongruenz $x^{p^\alpha-1} \equiv 1 \pmod{p^\alpha}$ hat genau $p-1$ Wurzeln, nämlich je eine aus jeder Restklasse \pmod{p} . Also gilt, wenn der Modul eine Primzahlpotenz ist, die FERMATSche Kongruenz nur bei sehr wenigen primen x .

2) Dasselbe Ergebnis hat Herr Prof. BACHMANN nach einer neuen brieflichen Mitteilung direkt abgeleitet, ohne Untersuchung der Fälle, in denen die Kongruenz wenigstens für einige a erfüllt ist.

3) Amer. journ. of math. 1, 1878, p. 184, 289. Vgl. BACHMANN in der *Enzykl. der math. Wissenschaften*, Bd. I, S. 576/7; ferner BACHMANN, *Niedere Zahlentheorie*, Bd. I (Leipzig 1902).

Teilbarkeit zu erkennen. Da aber die LEIBNIZsche Umkehrung unrichtig ist, so ist die von ihm daraus abgeleitete Methode zur Primzahlerkennung auch unrichtig, wie wir bald näher sehen werden.

Vorher haben wir uns noch mit einigen anderen zahlentheoretischen Untersuchungen zu beschäftigen, die LEIBNIZ in den achtziger Jahren des 17. Jahrhunderts angestellt hat und die zu dem FERMATSchen Satze in enger Beziehung stehen. In jener Zeit trat ihm nämlich das Problem der vollkommenen Zahlen nahe „ex M. JOH. WILH. PAULI Philintri (?) Lips. de num. perf. Lipsiae 1678“, einer mir unbekannten Schrift. (Handschrift 15.) Dies Problem steht zum FERMATSchen Satze in Beziehung, weil auch bei ihm ein Ausdruck der Form $2^n - 1$ die Hauptrolle spielt. Schon in Handschrift 16 kommt LEIBNIZ die Analogie in den Sinn: „ $2^{2^z+1} - 2^z$ erit numerus perfectus, si $2^{z+1} - 1$ est primitivus. Item $2^{z-1} - 1$ erit divisibile per z , si z est primitivus.“ Die Verbindung wird noch enger durch einen Satz, den LEIBNIZ beim „Philintrus“ (?) las: Die Summe der Glieder der geometrischen Reihe $1, 2, 2^2, \dots$ kann nur dann eine Primzahl sein, wenn die Gliederzahl eine Primzahl ist. Damit also $2^n - 1$ eine Primzahl (daher nach EUKLID $(2^n - 1) \cdot 2^{n-1}$ eine vollkommene Zahl) ist, muß n eine Primzahl sein. Aber wenn n eine Primzahl ist, so braucht $2^n - 1$ noch keine Primzahl zu sein. Primzahlen sind nach dem Philintrus (?) $2^2 - 1, 2^3 - 1, 2^5 - 1, 2^7 - 1, 2^{13} - 1, 2^{17} - 1, 2^{19} - 1$, und zu ihnen gehören daher 7 vollkommene Zahlen. Dagegen ist $2^{11} - 1$ teilbar durch 23, $2^{23} - 1$ teilbar durch 47 und $2^{41} - 1$ teilbar durch 83. Merkwürdigerweise haben alle drei Teiler von $2^n - 1$ die Form $2n + 1$. Diese Tatsache fand LEIBNIZ beim Philintrus (?) angegeben. Er legte sich nun die Aufgabe vor, den Grund für diese merkwürdige Teilbarkeiterscheinung zu finden.

Man sieht daraus, daß LEIBNIZ damals FERMATS 1679 erschienene *Varia opera mathematica* noch nicht kannte. Denn nach p. 163, 164, 177 dieser *Opera* hatte FERMAT schon 40 Jahre vor dem Philintrus (?) in Briefen an FRÉNICLE und MERSENNE hervorgehoben, was man bis dahin wohl nicht gewußt hatte¹⁾, daß $2^p - 1$ keine Primzahl zu sein brauche, wenn p es sei, und ferner noch, daß $2^p - 1$, wenn es keine Primzahl sei, lauter Primzahlteiler der Form $2lp + 1$ haben müsse. Er hatte dies aus seinem Satze gefolgert: Wenn $2^p \equiv 1 \pmod{p_1}$ ist, so ist p ein Teiler von $p_1 - 1$ oder umgekehrt $p_1 = kp + 1$. Wenn aber p eine ungerade Primzahl ist, so muß k eine gerade Zahl $2l$ sein, weil sonst $kp + 1$ eine gerade Zahl sein würde. Also hat jede Primzahl, die $2^p - 1$ teilt, die Form $2lp + 1$.

1) STIFEL hatte in der *Arithmetica integra* (1544), Bl. 10v, gemeint, $2^n - 1$ sei für alle ungeraden n eine Primzahl. Dieselbe Meinung hatte TARTAGLIA im *General trattato di numeri, et misure* II (1556), Bl. 146v, ausgesprochen.

Daß ferner $l = 1$ ist, daß also der Teiler von $2^p - 1$ die Form $p_1 = 2p + 1$ hat oder umgekehrt $2^{\frac{p_1-1}{2}} \equiv 1 \pmod{p_1}$ ist, tritt nach FERMAT, p. 164, z. B. ein, wenn $p_1 = a^2 - 2$ ist, also wenn 2 (nach späterer Ausdrucksweise) quadratischer Rest $\pmod{p_1}$ ist. Dies ist z. B. bei $p_1 = 23 = 5^2 - 2$ der Fall, und so erklärt sich die merkwürdige Erscheinung, daß $2^{11} \equiv 1 \pmod{23 = 2 \cdot 11 + 1}$ ist.

Als LEIBNIZ später FERMATS Werke studierte, hatte er die Fragestellung, auf die ihn die Lektüre des Philinrus (?) geführt hatte, längst vergessen, oder jedenfalls kam ihm der Zusammenhang nicht zum Bewußtsein. Und als er in noch späteren Jahren wieder einmal auf die vollkommenen Zahlen zurückkam (Handschrift 31, 32, 34.), war ihm das früher Gelesene sogar so vollständig aus dem Gedächtnis entschwunden, daß er jetzt wieder zu der längst widerlegten Meinung zurückkehrte, $2^p - 1$ müsse immer eine Primzahl sein, wenn p es sei. In Handschrift 31 äußert er diesen Satz als bloße Vermutung, sucht ihn aber in Handschrift 32 und 34 (Blatt 28, Rückseite) sogar durch eine unerlaubte „*conversio per contrapositionem*“ zu beweisen ($2^{p^q} - 1$ und $2^{p^r} - 1$ haben den gemeinsamen Teiler $2^p - 1$. Überhaupt geht der Teilbarkeit des Exponenten n immer die Teilbarkeit von $2^n - 1$ parallel. Also wird, so meint LEIBNIZ, auch der Primzahlcharakter von n und von $2^n - 1$ immer miteinander verbunden sein.) LEIBNIZ hätte gern eine vollständige Analogie der Sätze hergestellt: Stets dann, und nur dann, wenn p eine Primzahl ist, ist $2^{p-1} - 1$ durch p teilbar und $2^p - 1$ eine Primzahl. In Wirklichkeit ist aber im ersten Falle das „nur“ und im zweiten Falle das „stets“ falsch.

Das Problem der vollkommenen Zahlen hat uns auf die Frage nach der Bekanntheit LEIBNIZENS mit *Varia opera mathematica PETRI DE FERMAT* (Tolosae 1679) geführt, und es scheint mir jetzt an der Zeit, die Frage nach der Abhängigkeit der zahlentheoretischen Studien LEIBNIZENS von denen FERMATS aufzuwerfen. Daß LEIBNIZ FERMATS Werke nicht nur dem Namen nach gekannt, sondern selbst studiert hat, geht aus den Auszügen hervor, die er sich daraus angefertigt hat. (Handschrift 17.) Der FERMATSche Satz heißt in den *Varia opera* (p. 163): Tout nombre premier mesure infailliblement une des puissances $- 1$ de quelque progression que ce soit, et l'exposant de ladite puissance est sous-multiple du nombre premier donné $- 1$. Genau so, abgesehen von der Rechtschreibung, hat LEIBNIZ den Satz in seinen Auszügen auf Blatt 24 aufgeschrieben. Nur zu dem Worte „progression“ hat er, seiner gewohnten Ausdrucksweise entsprechend, das Wort „géometrique“ hinzugefügt.

Was ergibt sich nun hieraus für die Beantwortung der Frage, ob LEIBNIZ diesen Satz völlig selbständig neugefunden oder die Formulierung von FERMAT

übernommen und zu dem Übernommenen nur einen eigenen Beweis hinzugefügt hat? Wie mir scheint, gar nichts.¹⁾ Denn diese Auszüge sind leider undatiert, und wenn auch die Werke schon 1679 erschienen sind, so läßt sich daraus nicht schließen, daß LEIBNIZ sie schon vor dem 12. Sept. 1680 — dem Tage, an dem er den ersten Beweis des Satzes fand — kennen gelernt habe. Denn bis zum Bekanntwerden wissenschaftlicher Werke vergingen damals oft mehrere Jahre, und ausländische Bücher gar gelangten kaum nach Deutschland, wenn die Verfasser sie nicht selbst an bekannte Gelehrte schickten. Doch auch im letzteren Falle dauerte es beträchtliche Zeit, bis die Sendung überkam — wenn sie überhaupt je ihr Ziel erreichte.²⁾

Die Frage nach der Abhängigkeit muß also aus andern Gründen entschieden werden. CANTOR³⁾ will aus den Worten der *Nova algebrae promotio*⁴⁾ schließen, daß LEIBNIZ von FERMATS Vorwegnahme des Satzes nichts gewußt habe. Daß diese Folgerung unrichtig ist, zeigen die besprochenen Auszüge. Wenn man genau zusieht, so schreibt sich LEIBNIZ an dieser Stelle auch gar nicht die Urheberschaft des Satzes zu, der schon bei FERMAT zu finden ist, sondern darauf tut er sich etwas zugute, daß er hieraus zum ersten Mal eine *allgemeine Primzahlgleichung* abgeleitet habe. In der Tat mußte ja, wenn man dies Ziel erreichen wollte, zu dem von FERMAT Geleisteten noch Verschiedenes hinzugefügt werden. Es mußte zunächst aus den verschiedenen Möglichkeiten, die der Satz in der FERMATSchen Form zuläßt, die herausgesucht werden, die für alle Primzahlen gilt: $2^{x-1} = nx + 1$. Ferner mußte umgekehrt gezeigt werden, daß diese Gleichung nur für Primzahlen bestehen könne. Und drittens mußte eine Methode abgeleitet werden, um das Erfülltsein einer Gleichung von dieser Form, die von der früheren Mathematik noch nicht behandelt war, auch bei größeren Zahlen x festzustellen. Nun ist ja in der Tat die Umkehrung des FERMATSchen Satzes zuerst — wenn auch unrichtig — von LEIBNIZ ausgesprochen und zu beweisen gesucht worden, und LEIBNIZ ist auch der erste gewesen, der aus seinem *Exponential-*

1) Nur auf LEIBNIZENS Charakter fällt auch von hier aus ein merkwürdiges Licht. Denn er hat trotz seines Wissens um die Priorität FERMATS diesen nie erwähnt, und selbst in der *Nova algebrae promotio* (*LEIBNIZENS Math. Schr.* VII, 180—181), wo er seine eigenen Verdienste auf diesem Gebiete so stark hervorhebt, des großen Vorgängers mit keiner Silbe gedacht.

2) Aus dem Briefwechsel mit NICOLAS REMOND und REMOND DE MONTMORT (*LEIBNIZENS philosophische Schriften*, herausgegeben von C. I. GERHARDT III, 618, 666, 667) sowie mit NIK. BERNOULLI (*Math. Schr.* III, 985, 987) ersieht man z. B., welche Mühe es machte bis LEIBNIZ die 2. Auflage von R. DE MONTMORTS *Essai d'analyse sur les jeux de hasards* erhielt, dessen 1. Auflage unterwegs verloren gegangen war.

3) *Vorl.* III², 331.

4) „Hinc tandem duci potest aliquid hactenus analyticis incognitum, æquatio nempe generalis pro numero primitivo.“ *LEIBNIZENS Math. Schr.* III, 180—181.

kalkül eine Methode zur Behandlung derartiger Gleichungen abgeleitet hat. Er war also ganz berechtigt zu schreiben: „hinc mirum non est neminem prius dedisse æquationem generalem experimentem naturam numeri primitivi: nam nos ipsi primum hoc æquationum transcendentium genus in analysin introduximus.“¹⁾ LEIBNIZ schrieb sich also nur, und zwar mit Recht, die Urheberschaft der allgemeinen Primzahlgleichung und des Exponentialkalküls zu. Wer den ursprünglichen zahlentheoretischen Satz entdeckt habe, sagt er nicht. Es wäre ihm fast zuzutrauen, daß er hierüber absichtlich geschwiegen habe, um nicht gestehen zu müssen, daß ihm hierin ein andrer zuvorgekommen sei.

Jedenfalls läßt sich auch aus diesen Überlegungen nichts darüber erschließen, ob LEIBNIZ FERMATS Satz schon vor 1680 aus den Schriften des ersten Entdeckers gekannt hat. Es sind nun aber andre Gründe dafür vorhanden, daß LEIBNIZ tatsächlich diesen Satz unabhängig wiedergefunden hat, ehe er die *Varia opera* studierte. Denn die obige biographisch-geschichtliche Darstellung zeigt ja, daß LEIBNIZ spezielle Fälle des FERMATSchen Satzes schon 1676 gekannt hat. Der Gedankengang aber, der zur allgemeinen Entdeckung

1) LEIBNIZ beruft sich in dem jetzt folgenden Zitat zum Beweis hierfür auf einen Aufsatz in den *Acta eruditorum*, in dem er seinen „Ausdruck der Größe des Kreises durch die einfachste Reihe“ veröffentlicht habe, und auf seinen Nachweis, daß man Gleichungen, die „nicht von bestimmtem Grade“ seien, in der Geometrie nicht ausschließen könne. Ich kann im Augenblick nicht feststellen, welche der Aufsätze aus den Jahren 1682, 1684, 1691, 1693, 1695 LEIBNIZ hier im Auge hat. — Übrigens hatte er sich mit der Exponentialfunktion a^x schon 1679 beschäftigt und in Briefen an HUYGENS (*LEIBNIZENS Math. Schr.* II, 53, 56; *Der Briefwechsel von LEIBNIZ mit Mathematikern*, herausg. von C. I. GERHARDT, I, 568) Gleichungen der Form $x^2 + z^x = b$, $x^x + z^z = c$, $x^x - x = 24$ erwähnt. 1694 schrieb JOH. BERNOULLI ihm von seiner Entdeckung der „curvae percurrentes“, in deren Gleichung der Exponent alle Werte durchlaufe und zu denen der Logarithmus durch die Gleichung $a^{\log x} = x$ gehöre. (*LEIBNIZENS Math. Schr.* III, 139) LEIBNIZ antwortete, mit diesem Gebiete habe er sich schon in Briefen an HUYGENS und in seinen Aufsätzen der *Acta eruditorum* beschäftigt. Er nenne solche Kurven: „curvae exponentialiter transcendentis“. Sie seien leicht zu behandeln, wenn man ihre Verbindung mit den Logarithmen bemerke. (*LEIBNIZENS Math. Schr.* III, 141.) Im folgenden Jahre lehrte LEIBNIZ in seinem Aufsätze gegen NIEUWENTIJT die Differentiation der Exponentialfunktion mit Hilfe des Logarithmus genauer. (*Acta eruditorum* 1695; *LEIBNIZENS Math. Schr.* V, 325. JOH. BERNOULLI entdeckte, wohl unabhängig, die gleiche Formel und nahm sie in seinen Aufsatz über diesen Gegenstand (*Acta eruditorum* 1697, p. 125—133) mit auf, den er überschrieb: *Principia calculi exponentialium seu percurrentium*, indem er dabei der LEIBNIZschen Benennungsweise den Vorzug gab. Vgl. ferner TROPFKE, *Gesch.* I, 201—202; *Bibl. math.* 4₃, 1903, S. 217. Als *Kernpunkt des Ganzen* hatte LEIBNIZ mit Recht die *Beziehung zu den Logarithmen* bezeichnet. Denn man muß bedenken, daß die Logarithmen nicht als Potenzexponenten eingeführt waren, sondern als Glieder einer arithmetischen Reihe, die einer geometrischen zugeordnet ist. Erst EULER lehrte bekanntlich das Logarithmieren als 2. Umkehrung des Potenzierens auffassen.

führte, macht mit seiner allmählichen Vervollkommnung durchaus den Eindruck der Selbständigkeit. Zuerst wird aus den Perioden der Dualbrüche der zu weite Satz $a^k \equiv 1 \pmod{n}$ für beliebige Zahlen n abgeleitet, dann aus den Potenzsummenformeln ein zu enger Satz, der von Primzahlen p behauptet, $h = p - 1$ sei die niedrigste Potenz, für die $a^h \equiv 1 \pmod{p}$ werde. Und erst in noch späteren Handschriften, etwa Mitte der achtziger Jahre, ist der Satz vollständig richtig angegeben. Danach ist anzunehmen, daß LEIBNIZ FERMATS Werke erst etwa 1681 oder 1682 studiert und nur zur Vervollkommnung seines selbständig entdeckten Satzes benutzt hat. Hätte er sie schon vor 1680 gelesen, so würden sich wohl kaum solche ungenauen und unrichtigen Ausdrücke in seinen Formulierungen des Satzes finden, wie dies wirklich der Fall ist, es müßte denn sein, daß LEIBNIZ auch auf diesem Gebiete wie bei den vollkommenen Zahlen das bei FERMAT Gelesene so völlig vergessen hätte, daß eine gänzliche Neuentdeckung trotz der Lektüre nötig geworden wäre. Jedenfalls war er bei der Gewinnung des Satzes nicht bewußt von FERMAT beeinflusst.

Auch darauf mag noch einmal hingewiesen werden, daß auf einer der ersten Handschriften, die sich mit den vollkommenen Zahlen beschäftigen (Handschrift 16), der Satz sich schon notiert findet, während sich doch vorhin ergeben hatte, daß LEIBNIZ damals die Werke FERMATS wohl kaum gekannt hat. Er ist also vor dem Studium dieser Werke in Besitz des Satzes gewesen. — Höchstens das wäre noch denkbar, daß er in Paris etwa im Gespräche mit MARIOTTE (der freilich selbst nichts Genaues über zahlentheoretische Dinge gewußt zu haben scheint) etwas über FERMATS Entdeckung gehört (vgl. Handschrift 4) und dann selbständig versucht hätte, das Gehörte zur Genauigkeit und Exaktheit zu erheben. Völlig Gewisses und Bestimmtes — so muß ich diese Erörterung schließen — läßt sich über diesen Punkt nicht feststellen.

Auf alle Fälle ist es aber LEIBNIZENS Verdienst, als erster den Versuch gemacht zu haben, einen zahlentheoretischen Satz als notwendiges und hinreichendes Kriterium der Primzahlen aufzufassen und aus ihm ein Mittel zu deren Erkennung abzuleiten. Wie er das letztere ausgeführt hat, das will ich zum Schluß noch kurz skizzieren. Schon gleich bei Entdeckung der vermeintlichen allgemeinen Primzahlgleichung stellt er sich die Aufgabe: "Inquiramus, an ex mea primitivi proprietate reciproca aliquid ad praxin duci possit" (Handschrift 21). Die praktische Anwendbarkeit wird nämlich dadurch gefährdet, daß die Zahlen 2^x bei zunehmendem x zu stark wachsen, als daß man noch mit ihnen rechnen könnte. Um sich hier zu helfen, versucht LEIBNIZ schon in Handschrift 13 zwei Wege, deren Vereinigung ihn später tatsächlich zum Ziele gebracht hat: 1. Er bemüht sich, die Gleichung $2^{x-1} - 1 = nx$ mit Logarithmen zu behandeln, indem er sie als Exponentialgleichung nach Art der in den Briefen

an HUYGENS 1679 erwähnten¹⁾ auffaßt. 2. Er versucht statt mit den Potenzen mit ihren Resten nach verschiedenen Moduln zu rechnen.

Diese beiden verschiedenen Möglichkeiten, die ihm schon 1680 vorschwebten, hat er in den nächsten Jahren nach allen Seiten hin durchprobiert. Er schlägt vor, statt der gewöhnlichen Logarithmen, bei denen $\log 10 = 1$ ist, solche Logarithmen anzuwenden, bei denen $\log 2 = 1$ ist. Durch diese Logarithmen zur Basis 2 (wie wir heute sagen) würde die Rechnung erheblich vereinfacht werden, da hierbei $\log 2^x = x$ wäre. (Handschrift 22.) Er will ferner von 2^{p-1} ein möglichst großes Produkt, das den Faktor p enthält, abziehen (Handschrift 23, 24) oder statt dessen eine möglichst hohe Potenz von p (Handschrift 29, 1. Juni 1683), um dann nur noch den kleinen Rest auf seine Teilbarkeit durch p untersuchen zu müssen. Und um auch diese Subtraktion mit Logarithmen ausführen zu können, möchte er eine Regel finden, um aus den Logarithmen der Zahlen und der Differenz der Logarithmen den Logarithmus der Differenz ohne Benutzung der Zahlen zu finden (Handschrift 26, Juni 1682), und versucht diese Differenzlogarithmen aus der Logarithmusreihe abzuleiten. (Handschrift 28.)

Andererseits vereinfacht er sich das Rechnen mit den großen Zahlen, indem er an ihrer Stelle ihre Reste nach verschiedenen Moduln benutzt. In Handschrift 13 versucht er zuerst den Modul 10. Da für jedes $n: 2^{4n+1} - 1 \equiv 1$, $2^{4n+2} - 1 \equiv 3$, $2^{4n+3} - 1 \equiv 7$, $2^{4n+4} - 1 \equiv 5 \pmod{10}$ ist, so läßt sich der Rest von $2^{p-1} - 1$ bei Teilung durch 10 sofort angeben. Er sei $= r$. Andererseits ist der Rest von $p \pmod{10}$ gleich der letzten Ziffer von p . Er sei $= s$. Nun wäre zu untersuchen, ob eine Zahl mit dem Zehnerreste r durch eine Zahl mit dem Zehner s teilbar sein kann. Aber das läßt sich nur in besonderen Fällen (z. B. bei $s = 2$ oder 5) entscheiden. LEIBNIZ schlägt daher vor, andere Moduln zu nehmen, z. B. 9, d. h. mit Hilfe der Neunerprobe die Teilbarkeit festzustellen. (Handschrift 26, 27, 29.) Aber so kann man wohl die Nichtteilbarkeit, aber nicht die Teilbarkeit beweisen. LEIBNIZ nimmt daher zu dem Rest \pmod{n} , d. h. zur letzten Ziffer der Zahlen, wenn sie im Zahlensystem mit der Grundzahl n geschrieben werden, noch die vorangehenden Ziffern im n -adischen System hinzu und vergleicht diese bei $2^{p-1} - 1$ und p . (Handschrift 27.)

So wendet er die Grundgedanken hin und her, bis schließlich ihre folgende Kombination ihn zum Ziele führt: Er wählt x so, daß $2^x = y$ nur einen kleinen Rest \pmod{p} läßt. Da nun $x = \log y$ zur Basis 2 ist, so ändert sich x als Logarithmus additiv, wenn y sich multiplikativ ändert, dagegen multiplikativ, wenn y sich durch Potenzieren vergrößert. Man kann daher, wenn man 2^x bald durch Addition, bald durch Multiplizieren des Ex-

1) Siehe S. 56 Fußnote.

ponenten allmählich zu 2^{p-1} ansteigen läßt, entsprechend auch y durch Multiplizieren oder Potenzieren wachsen lassen. Um aber hier nicht zu große Zahlen zu erhalten, betrachtet man statt y, y_1, y_2, \dots, y_n nur die Reste von $y_n \pmod{p}$, die ja immer $< p$ sind. So erhält man schließlich den Rest von y_n , dem 2^{x_n} oder $2^{p-1} \pmod{p}$ kongruent ist, kann also feststellen, ob dieser Rest $= 1$ ist.

Aus dieser Überlegung hat LEIBNIZ in Handschrift 34—37 sein endgültiges Verfahren zur Primzahlerkennung abgeleitet, nachdem er es vielleicht in Handschrift 29 schon geahnt hatte.¹⁾ Er hat seiner Methode aus praktischen Gründen die Form eines Algorithmus gegeben, der ganz schematisch zum Ziele führt. Bei der Untersuchung des Primzahlcharakters von 101 wäre folgendermaßen zu verfahren: $101 - 1 = 100$. $100 : 2 = 50$. $50 : 2 = 25$. $25 - 1 = 24$. $24 : 2 = 12$. $12 : 2 = 6$. Weitere Verkleinerung ist nicht nötig, da $2^6 < 101$ ist. $2^6 = 64$. $2^{2 \cdot 6} = 64^2$, läßt also nach 101 den Rest 56. $2^{2 \cdot 12} = 56^2 = 5$. $2^{24+1} = 5 \cdot 2 = 10$. $2^{2 \cdot 25} = 10^2 = 100$. $2^{2 \cdot 50} = 100^2 = 1$. Also ist $2^{100} - 1$ durch 101 teilbar, daher ist 101 Primzahl (vorbehaltlich der Richtigkeit der Umkehrung des FERMATSchen Satzes). Man hat bei diesem Verfahren nur immer den Exponenten von 2 entweder um 1 wachsen zu lassen oder mit 2 zu multiplizieren und gleichzeitig die rechte Seite entweder in die 2. Potenz zu erheben oder mit 2 zu multiplizieren und jedesmal den Rest \pmod{p} festzustellen. Sobald einmal der Rest 1 auftritt, spätestens bei 2^{p-1} , ist dadurch p — meint LEIBNIZ — als Primzahl erwiesen.

Diese Methode ist natürlich deshalb unzureichend, weil aus $2^{p-1} = 1 \pmod{p}$ nur dann geschlossen werden darf, daß p Primzahl ist, wenn gleichzeitig bekannt ist, daß 2^h nicht $= 1 \pmod{p}$ für alle Teiler h von $p - 1$ ist. LEIBNIZ hätte also den Rest von 2^{p-1} auf dem Wege über sämtliche 2^h (bei 101 also auf dem Wege über $2^2, 2^4, 2^5, 2^{10}, 2^{20}, 2^{25}, 2^{50}$) finden müssen, und dann hätte zum ersten Male bei 2^{100} der Rest 1 kommen müssen. Wenn diese Bedingungen erfüllt gewesen wären, so hätte er mit Recht behaupten dürfen, daß 101 Primzahl sei. Wenn aber schon $2^h = 1 \pmod{p}$ geworden wäre, so hätte er nicht mit Recht behaupten können, daß p keine Primzahl sei, sondern hätte eine andere Basis versuchen müssen und vielleicht noch eine dritte und vierte. So wird das Verfahren, wenn man nicht gleich die richtige Basis (eine primitive Wurzel der Primzahl) trifft, sehr umständlich, und auch bei geeigneter Wahl der Basis ist es unter Umständen gar nicht ausführbar, wenn man die Teiler von $p - 1$ nicht kennt.

Trotzdem ist die LEIBNIZsche Methode nicht uninteressant, da sie eben der erste Versuch auf diesem Gebiete gewesen ist und viele gute Gedanken

• 1) LEIBNIZ hat seinen Gedankengang in Handschrift 29 nur so kurz und flüchtig angedeutet, daß dieser nicht ganz verständlich ist. Ich wüßte aber nicht, worauf sich seine Worte: „Hic tandem arcanum illud detectum videtur“ anders beziehen sollten als auf die Methode der Primzahlerkennung.

zur Praxis des zahlentheoretischen Rechnens enthält. Als Kernpunkt des Verfahrens hat LEIBNIZ selbst erklärt, daß hier mit den Potenzresten statt mit den Potenzen selbst auf Grund einer quasi-logarithmischen Beziehung zwischen beiden gerechnet werde.¹⁾ Diese Beziehung ist zunächst nur äußerlich der logarithmischen verwandt, nur „quasi-logarithmisch“, indem sie nämlich gestattet mit kleineren Zahlen (den Potenzresten) statt größerer (den Potenzen selbst) zu rechnen, auf Grund der Regeln: Das Produkt der Reste zweier Zahlen läßt denselben Rest wie das Produkt der Zahlen, und die Potenz des Restes einer Zahl läßt den gleichen Rest wie die Potenz der Zahl (überall der gleiche Modul vorausgesetzt.²⁾ Die Beziehung steht aber noch unmittelbarer mit dem Logarithmus in Verbindung: *Si exponentium augmenta sint ut logarithmi, residuorum multiplicationes sunt ut numeri progressionis geometricae.* (Handschrift 34.) Wenn die Exponenten in arithmetischer Reihe zunehmen, so die Potenzen in geometrischer, und der Addition der Exponenten entspricht die Multiplikation der Reste. Auf diese logarithmische Beziehung ist bekanntlich später, indem man als Basis eine primitive Wurzel nahm, das Indexrechnen gegründet worden, das in der Zahlentheorie eine ähnliche Stelle einnimmt wie das Logarithmenrechnen in der Arithmetik. LEIBNIZ allerdings hatte von dieser Beziehung keinen Vorteil, da er durch sie genötigt war zu multiplizieren statt zu addieren, während man beim Indexrechnen addiert statt zu multiplizieren.

Nachdem LEIBNIZ die eben geschilderte Methode der Primzahlerkennung ausgebildet hatte, hielt er das Gebiet für einstweilen abgeschlossen und bereitete eine zusammenfassende Abhandlung vor. Er glaubte durch seine Umkehrung des FERMATSchen Satzes einen „*Novus aditus ad incognita hactenus mysteria numerorum*“ gefunden zu haben (Handschrift 33) und durch seine Exponentialgleichung der Primzahlen auch diese Probleme „in die Gewalt der Analytiker“ gebracht zu haben, während noch DESCARTES habe gestehen müssen, daß sein Können hier nicht ausreiche. Die Handschrift 33, die mit der Erwähnung der von LEIBNIZ gefundenen allgemeinen Primzahlgleichung schließt, ist als Einleitung der geplanten Abhandlung aufzufassen, von der ein größerer Entwurf unter dem Titel „*Inqvisitio in numeros primitivos et derivatorum divisores*“ (Handschrift 34) erhalten ist.

Warum aber hat LEIBNIZ trotz dieses ziemlich weit gediehenen Entwurfes, bei dem er sicher an den Druck gedacht hat, über den Gegenstand

1) *Opus est modo commodo investigandi residuos altissimarum potentiarum, quas ipsas habere et dividere non licet. Eum vero praebet residuorum relatio quasi logarithmica inter se, ad instar ipsorum potentiarum, ita ut factum ex duobus residuis idem praebet residuum, quod praebet factum ex ipsis numeris.* (Handschrift 30).

2) LEIBNIZ schreibt diese Regeln in Handschrift 34: $R(mRf) = R(mf)$, wobei m kleiner als der Modul angenommen ist; $R((Rf)m) = R(f^m)$.

garnichts veröffentlicht? Sollten ihm doch Bedenken über die Tragweite seiner Beweise und die praktische Anwendbarkeit seiner Methoden gekommen sein? Man könnte es fast denken. Denn in den *Nouveaux essais sur l'entendement humain*³⁾ (1704) erklärt er, als wenn er selbst auf diesem Gebiete garnichts geleistet hätte, die Mathematiker suchten noch immer vergeblich nach einem Merkmale, das sie dazu befähige, eine vorgelegte Zahl leicht und sicher als Primzahl zu erkennen.

So ist die LEIBNIZSCHE allgemeine Primzahlgleichung ein ungeborener geistiger Embryo geblieben. Aber ich glaube gezeigt zu haben, daß schon die Untersuchung der Entwicklung dieses nie geburtsreif gewordenen Gedankens von Wert für die Geschichte und Psychologie des mathematischen Denkens ist. Noch viel mehr würde es sich lohnen, die großen Entdeckungen, die LEIBNIZ zum Mitbegründer einer neuen Periode in der Geschichte der Wissenschaft gemacht haben, in ihrer vorgeburtlichen Entwicklung nach den Handschriften der hannoverschen Bibliothek zu studieren. Auch über die von mir nur kurz gestreiften Gebiete: harmonisches Dreieck (in seiner Beziehung zur Entdeckung der Differentialrechnung), polynomischer Lehrsatz, Potenzsummenformeln, periodische Dezimalbrüche, Irrationalität von π , Exponentialfunktion und Logarithmus, ließe sich sicher noch manches aus den LEIBNIZSCHEN Papieren feststellen. Doch das wäre eine Aufgabe, die ich Kundigeren überlassen muß. Mir war schon diese kleine Arbeit eine schwere Mühe, da ich, als ich zufällig auf sie geführt wurde, weder über das behandelte Gebiet der Mathematik, noch über die Geschichte dieses Gebietes unterrichtet war.

1) Buch 4, Kap. 17, § 13.