# Über die Faktorenzerlegung natürlicher Zahlen

Autor(en): **Finsler, P.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **2 (1947)**

Heft 1

PDF erstellt am: **01.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-12812

# ELEMENTE DER MATHEMATIK

Revue de mathématiques élémentaires — Rivista di matematica elementare

*Zeitschrift zur Pflege der Mathematik*
*und zur Förderung des mathematisch-physikalischen Unterrichts*
*Organ für den Verein Schweizerischer Mathematiklehrer*

El. Math. Band II Nr. 1 Seiten 1–24 Basel, 15. Januar 1947


## Über die Faktorenzerlegung natürlicher Zahlen

Es ist eine besonders wegen ihrer Schwierigkeit reizvolle Aufgabe, gegebene, nicht zu kleine natürliche Zahlen in ihre Primfaktoren zu zerlegen. Man kommt zwar bei jeder Zahl «mit endlich vielen Schritten» zum Ziel, man muß ja nur die Primzahlen, welche die Quadratwurzel der gegebenen Zahl nicht übertreffen, der Reihe nach als Teiler durchprobieren; wenn keine der Divisionen aufgeht, so ist die Zahl selbst eine Primzahl, andernfalls hat man einen Primteiler gefunden und kann den Quotienten in gleicher Weise behandeln. Bei größeren Zahlen kann aber dieses Verfahren ohne besondere Hilfsmittel sehr langwierig und deshalb undurchführbar werden.

Soweit Faktorentafeln zur Verfügung stehen, wird man diese verwenden; es genügt dabei, wenn aus der Tafel jeweils der kleinste Primteiler einer Zahl ersichtlich ist, sofern die Tafel zu jeder Zahl auch alle kleineren enthält. Es gibt solche Tafeln, die bis zu zehn Millionen reichen[1]). Da aber diese Tafeln nicht immer gerade zur Hand sein werden, können auch für kleinere Zahlen noch andere Methoden nützlich sein.

Anstatt direkt die Teiler zu suchen, kann man auch die möglichen Darstellungen der gegebenen Zahl als Summe oder als Differenz von Quadraten zu bestimmen suchen und hieraus unter Umständen auf die Teiler schließen. Bildet man zum Beispiel die Summe $n + 1 + 3 + 5 + 7 + \cdots$ und gelangt dabei nach $y$ Schritten zur Zahl $x^2$, so ist $n = x^2 - y^2$, und man erhält die Zerlegung $n = (x - y)\ (x + y)$. Ohne ein Durchprobieren wird man aber im allgemeinen nicht auskommen. Die Aufgabe besteht darin, dieses Durchprobieren möglichst rationell zu gestalten. Dazu kann man entweder die Anzahl der Versuche einschränken, indem man etwa mit zahlentheoretischen Methoden, insbesondere mit der Theorie der quadratischen Reste, alle Zahlen, die bestimmten Formen angehören, als Lösungen ausschließt[2]), oder man kann auch mit elementaren Mitteln versuchen, die nötigen Operationen so zu vereinfachen, daß sie sich ohne Mühe rasch durchführen lassen. Im folgenden soll gezeigt werden, wie dies durch eine Kombination der Division von links nach dem Prinzip des Rechenschiebers mit einer arithmetischen Division von rechts geschehen kann. Nur die kleinsten Primfaktoren sind noch besonders zu betrachten.

### 1. *Teilbarkeitsregeln*

Es ist wichtig, zunächst die kleinsten Faktoren zu prüfen, denn die Wahrscheinlichkeit, daß eine Division aufgeht, ist um so größer, je kleiner die Zahl der möglichen

[1]) D. N. Lehmer, Factor Table for the first ten millions (Washington 1909).

[2]) Ausführliche Darstellung bei M. Kraitchik, Théorie des nombres I, II (Paris 1922, 1926), Recherches sur la théorie des nombres I, II (Paris 1924, 1929). Vgl. auch Leonhard Euler, Opera omnia, insbes. Ser. I, Bd. 3 und 4.

Reste, je kleiner also der Teiler ist. Außerdem können manche Methoden in solchen Fällen, wo der zweite Faktor sehr groß wird, versagen.

Die Teilbarkeit einer Zahl durch 2 oder 5 ist sofort an der letzten Ziffer, die Teilbarkeit durch 3 (oder 9) an der Quersumme zu erkennen. Auch für die Teilbarkeit durch 11 gibt es eine bekannte Regel. Weniger bekannt sind solche Regeln für die Zahlen 7 oder 13. Man kann zwar zeigen, daß es zu jeder Primzahl eine «Teilbarkeitsregel» geben muß; diese haben aber meist den Nachteil, daß man sie leicht vergißt, und sie sind auch für größere Primzahlen weniger rationell. Nützlich ist jedoch eine Regel, welche die Teiler 7, 11 und 13 zugleich erfaßt[1]):

Man teile die im Dezimalsystem geschriebene Zahl wie üblich von rechts nach links in Gruppen von je 3 Ziffern ein, deute diese Gruppen als dreistellige Zahlen und bilde die Summe der ersten, dritten, fünften usw. sowie die der zweiten, vierten, sechsten usw. dieser Zahlen. Die Differenz der beiden Summen ist dann und nur dann durch 7, 11 oder 13 teilbar, wenn schon die ursprüngliche Zahl durch 7, 11 oder 13 teilbar ist.

Es folgt dies leicht, wenn man die gegebene Zahl durch $1001 = 7 \cdot 11 \cdot 13$ dividiert. Nach ein- oder zweimaliger Anwendung der Regel erhält man eine (höchstens) dreistellige Zahl. Es gilt dann noch die Zusatzregel:

Eine dreistellige Zahl ist durch 11 teilbar, wenn die Summe der ersten und letzten Ziffer, vermindert um die zweite Ziffer, 0 oder 11 ergibt; um die Teilbarkeit durch 7 oder 13 zu prüfen, kann man von der ersten und letzten Ziffer gleichzeitig ebensoviel wegnehmen, als man zur mittleren Ziffer hinzufügt, um so eine zweistellige Zahl oder das Zehnfache einer solchen zu erhalten; diese ist durch 7 oder 13 teilbar, wenn die ursprüngliche Zahl durch 7 oder 13 teilbar ist.

Der erste Teil des Satzes ergibt sich aus der gewöhnlichen Elferregel, der zweite aus der Beziehung $7 \cdot 13 = 91 = 101 - 10$. Bei einer zweistelligen Zahl ist die Teilbarkeit durch 7 oder 13, evtl. nach Abspaltung eines kleineren Faktors, sofort ersichtlich; bei der Zahl 91 könnte man die Regel nochmals anwenden, um 0 zu erhalten. Es lohnt sich, die Regeln zu behalten; sie sind nicht bequem zu beschreiben, aber einfach anzuwenden. Die Zahl 1946 zum Beispiel ist durch 7, aber nicht durch 13 teilbar, denn man erhält $946 - 1 = 945$, $945 - 505 + 050 = 490$ und $49 = 7 \cdot 7$.

Nachdem die Primfaktoren bis zu 13 beseitigt sind, kann die weitere Prüfung von Teilern mit der Zahl 17 beginnen. Alle Zahlen unterhalb $17^2 = 289$, bei denen die genannten Regeln keinen Faktor ergeben, sind Primzahlen, so zum Beispiel die Zahlen 17 und 107.

Den Teilbarkeitsregeln entsprechen gewisse Rechenproben; insbesondere wird die bekannte Neuner- und Elferprobe im folgenden gebraucht.

## 2. *Verwendung des Rechenschiebers*

In der Normallage eines logarithmischen Rechenschiebers stehen sich bei beliebig verschobener Zunge in den Skalen gleicher Längeneinheit Zahlen gegenüber, die ein festes Verhältnis besitzen. Zieht man die Zunge des Schiebers heraus und führt sie in umgekehrter Richtung wieder ein, so daß die Skalen in entgegengesetztem Sinne verlaufen, so haben gegenüberstehende Zahlen der Skalen gleicher Längen-

[1]) Diese Regel findet sich gelegentlich in der Literatur, so z. B. bei L. LOCHER, Arithmetik und Algebra (1945), Kap. 33; die ziemlich notwendige Zusatzregel konnte ich bisher nirgends finden.

einheit ein konstantes Produkt. Zum Ablesen muß der Läufer benutzt werden, da die Skalen nicht mehr direkt aneinanderliegen. Bei Schiebern mit Reziprokteilung kann diese verwendet werden.

Stellt man nun die Zahl 1 der Zahl $n$ gegenüber und ist $n = p \cdot q$, so müssen sich auch die Zahlen $p$ und $q$ gegenüberstehen. Ist zum Beispiel $n = 1007$, so sieht man, daß die Zahlen 19 und 53 einander gegenüberstehen, und findet so die Zerlegung $1007 = 19 \cdot 53$.

Allgemein wird man also, wenn die Zahl $n$ zu untersuchen ist und keine kleineren Primfaktoren als 17 vorhanden sind, den Schieber so einstellen, daß das konstante Produkt gleich $n$ wird, sodann auf der einen Skala die Primzahlen von 17 ab mit dem Läufer verfolgen und auf der andern Skala nachsehen, ob eine ganze Zahl mit richtiger Stellenzahl gegenübersteht. Solange dies nicht der Fall ist, geht man weiter; wenn es aber mit hinreichender Genauigkeit der Fall ist, müssen die Zahlen schärfer geprüft werden. Dabei wird man besonders auf die Endziffern achten. Da die Faktoren 2 und 5 ausgeschaltet sind, kommen nur die Endziffern 1, 3, 7 und 9 in Frage, und zwar für die Zahl $q$ bei gegebenen Zahlen $n$ und $p$ nur eine bestimmte davon. Da die letzte Ziffer von $n$ bekannt ist, kann man sich eine kleine Tabelle anlegen, welche die möglichen Endziffern von $p$ und $q$ einander gegenüberstellt. Ist zum Beispiel die letzte Ziffer der Zahl $n$ eine 7, so erhält man die Zuordnung $\begin{array}{|c|c|c|c|}\hline 1 & 3 & 7 & 9 \\ \hline 7 & 9 & 1 & 3 \\ \hline \end{array}$.

Wenn bei der Ablesung auf dem Schieber die Endziffer von $q$ nicht stimmt, geht man weiter; wenn sie stimmt (oder wenn sie bei Interpolation mit hinreichender Genauigkeit stimmen kann), so macht man die Neuner- und eventuell die Elferprobe, wofür man sich den Neuner- und den Elferrest der Zahl $n$ von vornherein notieren wird. Wenn beide Proben stimmen, kann man bei nicht zu großen Zahlen sicher sein, eine Zerlegung gefunden zu haben, und wird dies nur noch zur Kontrolle durch direktes Ausrechnen bestätigen. Wenn sich aber für alle Primzahlen $p$ bis zu $\sqrt{n}$ kein passender Faktor $q$ ergibt, so ist $n$ selbst eine Primzahl.

Die Prüfung der Einzelfälle ist meistens so einfach, daß man die Zahl $p$ nur so lange auf die Primzahlen beschränkt, als man diese auswendig kennt, dann aber alle Zahlen mit den Endziffern 1, 3, 7, 9 durchlaufen läßt, sofern man nicht schon sieht, daß sie etwa durch 3 oder 7 teilbar sind. Auch bei der gegenüberstehenden Zahl $q$ wird man häufig bemerken, daß sie durch 3 teilbar ist, und kann dann sofort weitergehen.

Ist etwa $n = 10007$, so findet man zunächst keinen Teiler kleiner als 17. Man stellt nun auf dem Rechenschieber die letzte 1 der Zunge der Zahl 10007, also praktisch der ersten 1 des Stabes gegenüber. Man hat bei dieser Zahl den Vorteil, die längere Skala des gewöhnlichen Rechenschiebers ohne Durchziehen in einer Stellung ausnutzen zu können; man kann aber auch die kleinere Skala verwenden. Für $p$ kommen jetzt die Primzahlen von 17 bis 97 in Betracht und wegen der Endziffer 7 von $n$ gilt die obenstehende Zuordnung der Endziffern von $p$ und $q$. Man findet als «verdächtige» Faktoren zunächst etwa $37 \cdot 271$, wobei die Neunerprobe nicht stimmt, sodann $53 \cdot 189$, wobei der zweite Faktor durch 9 teilbar ist, also ebenfalls nicht in Betracht kommt. Andere Faktoren ergeben sich nicht, die Zahl 10007 ist Primzahl.

Wollte man die Zahl 100007 in gleicher Weise behandeln, so müßte man anfangs, da $q$ vierstellig wird und die vierte Stelle auf dem Rechenschieber nicht mehr genau

abzulesen ist, jedesmal die Neunerprobe anwenden. Dies läßt sich vermeiden, wenn man die Zuordnung der *zwei* letzten Ziffern von $p$ und $q$ in Betracht zieht; sie ist durch die beiden letzten Ziffern von $n$ festgelegt. Man erweitert also die frühere «einstellige» Tabelle zu einer «zweistelligen». Sind, wie im Beispiel, 07 die Endziffern von $n$, so entsprechen den Endziffern 01, 03, 07, 09, 11, 13, 17, ..., 97, 99 von $p$ die Endziffern 07, 69, 01, 23, 37, 39, 71, ..., 31, 93 von $q$. Man findet diese Werte leicht, indem man die Zahl $n$ (bzw. ihre letzten Stellen) von rechts her durch $p$ dividiert; die Division ist wegen der Endziffern 1, 3, 7, 9 des Divisors stets eindeutig. Es genügt jedoch, nur die vier ersten Zahlen der Reihe auf diese Weise zu bestimmen; nachher wiederholen sich die letzten Ziffern periodisch und die vorletzten Ziffern ergeben sich leicht, wenn man die Zahlen $p$ um je 10 vergrößert. Es gilt dann $(p+10) \times (q + 10x) \equiv pq \pmod{100}$, also, wenn $p_2$, $p_1$ bzw. $q_2$, $q_1$ die letzten Ziffern von $p$ und $q$ sind, $p_1 x + q_1 \equiv 0 \pmod{10}$. Bei festen Endziffern $p_1$, $q_1$ ist also $x$ eindeutig bestimmt, man erhält jedesmal eine arithmetische Progression. Für $p_1 = 1$, $q_1 = 7$ wird $x = 3$, den Endziffern 01, 11, 21, 31, 41, 51, ... von $p$ entsprechen also im Beispiel die Endziffern 07, 37, 67, 97, 27, 57, ... von $q$, den Endziffern 03, 13, 23, 33, 43, 53, ... von $p$ mit $x = 7$ die Endziffern 69, 39, 09, 79, 49, 19, ... von $q$ usf. Die ganze Tabelle läßt sich auf diese Weise rasch anschreiben. Vergleicht man jetzt auf dem Rechenschieber die den Primzahlen $p$ gegenüberstehenden Werte mit der Tabelle, so findet man eine erste Übereinstimmung bei den Faktoren $97 \cdot 1031$. Die Neuner- und die Elferprobe stimmen, man hat also die Zerlegung gefunden:

$$100007 = 97 \cdot 1031.$$

Will man noch größere Zahlen behandeln, so kann man die drei letzten Stellen von $p$ und $q$ einander zuordnen, also eine «dreistellige» Tabelle benutzen. Auch diese läßt sich leicht herstellen, wenn man berücksichtigt, daß jetzt ein stetes Fortschreiten um 10 bei $p$ eine Progression zweiten Grades für $q$ ergibt, während ein Fortschreiten um 100 wieder eine leicht zu findende Progression ersten Grades liefert, bei der die beiden letzten Stellen von $q$ sich nicht ändern. Man kann also der Tabelle zum Beispiel für die Endziffern 007 von $n$ die folgende Form geben, wobei links die zwei letzten Ziffern $p_2$, $p_1$ von $p$ stehen, oben die drittletzte Ziffer $p_3$ von $p$, ganz rechts die zwei letzten Ziffern $q_2$, $q_1$ von $q$ und dazwischen die drittletzte Ziffer $q_3$ von $q$:

$n = \ldots 007$

| $p$ | 0123456789 | $q$ |
|---|---|---|
| 01 | 0369258147 | 07 |
| 03 | 6307418529 | 69 |
| 07 | 0741852963 | 01 |
| 09 | 2581470369 | 23 |
| 11 | 6925814703 | 37 |

usw.

Es ist zweckmäßig, sich vertikale Streifen herzustellen, auf denen die Primzahlen $p$ durch ihre Neunerreste markiert sind und die man an die entsprechenden Kolonnen für $q_3$ anlegen kann; wenn man bei der Vergleichung mit dem Rechenschieber für die Endstellen von $q$ Übereinstimmung findet, macht man die Neunerprobe. An-

fangs, das heißt für kleinere Werte von $p$, ist größere Vorsicht nötig, später geht das Vergleichen sehr rasch.

Für die Zahl 1000007 findet man bald die Zerlegung

$$1000007 = 29 \cdot 34483.$$

Daß der zweite Faktor eine Primzahl ist, kann daraus entnommen werden, daß sich bei Verwendung derselben Tabelle und derselben Einstellung für die Primzahlen von 31 bis 181 und auch für die Zahl $29^2 = 841$ keine Übereinstimmung mehr findet.

Dieselbe Tabelle kann auch noch zur Prüfung der Zahl 10000007 verwendet werden. Daß man hier öfters die Neunerprobe verwenden muß, spielt jetzt im Verhältnis zur Gesamtzahl keine große Rolle mehr. Da die fraglichen Zahlen $q$ durch den Rechenschieber und die Tabelle vollständig gegeben sind, braucht man sie bis zum Endergebnis nicht zu notieren. Man findet die Zerlegung:

$$10000007 = 941 \cdot 10627.$$

Wenn man viele verschiedene Zahlen zu behandeln hat, ist es zweckmäßig, eine größere Tafel zu verwenden, welche für alle möglichen dreistelligen Endungen $n_3\, n_2\, n_1$ von $n$ und die Endungen $0\, p_2\, p_1$ von $p$ die zugehörigen dreistelligen Endungen $q_3\, q_2\, q_1$ von $q$ angibt. Man kann sie in gleicher Weise anordnen, wie die frühere; wieder stehen links die Zahlen $p_2 p_1$, rechts die Zahlen $q_2 q_1$, dazwischen $q_3$, nur oben steht an Stelle von $p_3$ jetzt die Ziffer $n_3$. Da wieder einfache Progressionen bestehen, läßt sich die Tafel ohne große Mühe herstellen, worauf aber hier nicht näher eingegangen werden soll. Für die Endungen $n_3 07$ von $n$ ergibt sich folgendes Bild:

$n = \ldots 07$

| $p$ | 0123456789 | $q$ | |
|---|---|---|---|
| 01 | 0123456789 | 07 | |
| 03 | 6307418529 | 69 | |
| 07 | 0369258147 | 01 | |
| 09 | 2109876543 | 23 | |
| 11 | 6789012345 | 37 | usw. |

Die ganze Tafel läßt sich auf 8 Seiten unterbringen. Sie liefert für jede zu untersuchende Zahl $n$ und für die Zahlen $p$ unter 100 die dreistelligen und für die größeren Zahlen $p$ die zweistelligen Endungen von $q$ direkt. Sucht man alle dreistelligen Endungen von $q$ zu gegebenem $n$, so ergibt sich jetzt die zugehörige Tabelle sehr leicht, da nur noch für die Ziffern $q_3$ einfache Progressionen mit bekannten Differenzen anzuschreiben sind, die sich nach je vier Zeilen periodisch wiederholen. Je nachdem $n_1$ gleich 1, 3, 7 oder 9 ist, haben diese Differenzen die Werte 9, 1, 1, 9; 7, 3, 3, 7; 3, 7, 7, 3; 1, 9, 9, 1. Eine vollständige dreistellige Tafel für alle Werte von $n$ und $p$ würde 80 Seiten beanspruchen.

Eine Vereinfachung ergibt sich, wenn über die Endziffern der Faktoren von $n$ schon von vornherein etwas bekannt ist. Dies ist bei Zahlen der Form $a^m \pm b^m$ der Fall, sofern $m$ durch 2 oder 5 teilbar ist; primitive Faktoren[1]) solcher Zahlen besitzen

[1]) Primitive Faktoren einer Zahl $a^m \pm b^m$ sind solche Primfaktoren, die nicht schon in einer Zahl $a^n \pm b^n$ mit $n < m$ aufgehen.

die Form $km + 1$. Unter Umständen kann man die Zahlen zunächst algebraisch zerlegen und dann die einzelnen Teile weiter untersuchen. So ist zum Beispiel $a^{10} + b^{10}$ durch $a^2 + b^2$ teilbar, und wenn speziell $a = x^2$, $b = 2y^2$ ist, so findet man mit $Q = (a^4 + a^3 b - a^2 b^2 + a b^3 + b^4)$, $R = 2xy(a^3 + b^3)$, $L = Q - R$, $M = Q + R$ die Zerlegung $a^{10} + b^{10} = (a^2 + b^2) \cdot L \cdot M$. Für $a = 25$, $b = 72$, also $x = 5$, $y = 6$ ergibt sich $L = 11148301$, $M = 57813061$. Diese Zahlen sind nun weiter zu untersuchen. Die Faktoren müssen hier die Form $2km + 1$ besitzen, sie können also nur auf 01, 21, 41, 61 oder 81 enden. Man kommt daher mit folgenden dreistelligen Tabellen aus:

$n = \ldots 301$

| $p$ | 0123456789 | $q$ |
|---|---|---|
| 01 | 3210987654 | 01 |
| 21 | 6543210987 | 81 |
| 41 | 8765432109 | 61 |
| 61 | 8765432109 | 41 |
| 81 | 6543210987 | 21 |

$n = \ldots 061$

| $p$ | 0123456789 | $q$ |
|---|---|---|
| 01 | 0987654321 | 61 |
| 21 | 2109876543 | 41 |
| 41 | 2109876543 | 21 |
| 61 | 0987654321 | 01 |
| 81 | 5432109876 | 81 |

Die Faktoren unter 1000 sind schon geprüft[1]); die größeren Faktoren kann man an Hand der Tabellen mit dem Rechenschieber untersuchen und findet: $L$ ist Primzahl, $M = 2381 \cdot 24281$. Wegen $25^2 + 72^2 = 37 \cdot 157$ folgt also die Zerlegung:

$$25^{10} + 72^{10} = 37 \cdot 157 \cdot 2381 \cdot 24281 \cdot 11148301 .$$

### 3. *Rechenwalze und Reziprokentafel*

Mit Hilfe einer Rechenwalze kann man in gleicher Weise noch größere Zahlen behandeln. Der Korb wird in umgekehrtem Sinne auf die Walze aufgeschoben, so daß auf den Skalen sich gegenüberstehende Zahlen wiederum ein konstantes Produkt ergeben. Bei einer Längeneinheit von 15 $m$ kann man vier Stellen direkt ablesen, die fünfte und eventuell sechste noch schätzen; man hat also etwa zwei Stellen mehr als beim gewöhnlichen Rechenschieber. Für eine bestimmte Zahl $n$ braucht man nur die eine Stellung, in welcher die Zahl 1 des Korbes der Zahl $n$ der Walze gegenübersteht.

Für kleine Werte von $p$ muß man bei großem $n$ sorgfältiger ablesen und eventuell die Neunerprobe verwenden; sobald aber $p$ größer und $q$ entsprechend kleiner geworden ist, geht die Ablesung im allgemeinen sehr leicht, und da sich schließlich die zu vergleichenden Werte auf der Walze nur noch langsam ändern, kommt man rasch vorwärts. Man muß ja meistens nur eine und nur in etwa einem Hundertstel der Fälle alle drei Ziffern vergleichen. So kann man zum Beispiel bei der Zahl $n = 100000007$ alle Zahlen $p$ bis zu 10000 durchnehmen, und da sich für die zugehörigen $q$ keine Übereinstimmung mit der dreistelligen Tabelle ergibt, findet man:

$$100000007 = \text{Primzahl}.$$

Wie die späteren Beispiele zeigen, können noch größere Zahlen mit der Rechenwalze behandelt werden. Bei Zahlen, die relativ sehr nahe bei einer Zehnerpotenz liegen, verwendet man jedoch zweckmäßiger eine Reziprokentafel, die ja dieselbe

[1]) Vgl. A. J. C. CUNNINGHAM, Binomial Factorisations II (London 1924), S. 183.

Zuordnung ergibt und eventuell noch mehr Stellen liefert. Mit einer Tafel, welche die Reziproken der Zahlen 1 bis 100 auf acht und die der Zahlen von 101 bis 10000 auf sieben geltende Stellen genau angibt[1]), findet man zum Beispiel noch die folgenden Resultate, wobei für die Zahlen $p$ von 10000 ab die Rechenwalze zu benutzen ist:

$$1000000007 = \text{Primzahl},$$
$$10000000007 = 23 \cdot 2293 \cdot 189613,$$
$$100000000007 = 353 \cdot 283286119.$$

Beim Aufsuchen der Faktoren kann man auf Zahlen stoßen, deren Produkt auf mehrere Stellen am Anfang und außerdem in den drei letzten Stellen mit der gegebenen Zahl übereinstimmt, bei denen aber die Neuner- oder Elferprobe oder auch eine kleine Differenz auf der Rechenwalze zeigt, daß es doch nicht die gewünschte Zahl ist. So findet man zum Beispiel an Stelle von 100000007 das Produkt $3251 \cdot 30757 = 99991007$, bei dem auch die Neunerprobe stimmt, oder bei dem letzten Beispiel, wo der zweite Faktor als Primzahl festzustellen ist, das Produkt $3847 \cdot 4481 \cdot 5801 = 99999999007$, das um genau 1000 zu klein ist.

Einer Tafel von M. KRAITCHIK, welche die kleinsten Primfaktoren der zwischen $10^{12}$ und $10^{12} + 10000$ gelegenen Zahlen angibt[2]), entnehme ich die Zerlegung:

$$1000000000007 = 34519 \cdot 28969553.$$

Um die Methode noch an weniger speziellen Zahlen zu prüfen, werde die Aufgabe betrachtet, die Zähler und Nenner der Näherungsbrüche $A_k : B_k$ zu zerlegen, die sich bei der Kettenbruchentwicklung der Zahl $\pi$ ergeben. Es ist

$$\pi = (3;\ 7,\ 15,\ 1,\ 292,\ 1,\ 1,\ 1,\ 2,\ 1,\ 3,\ 1,\ 14,\ 2,\ 1,\ 1,\ 2,\ 2,\ 2,\ 2,\ 1,\ \ldots),$$

und man findet (mit $P$ = Primzahl):

$A_1 = 3 = P,$ $B_1 = 1,$
$A_2 = 22 = 2 \cdot 11,$ $B_2 = 7 = P,$
$A_3 = 333 = 3^2 \cdot 37,$ $B_3 = 106 = 2 \cdot 53,$
$A_4 = 355 = 5 \cdot 71,$ $B_4 = 113 = P,$
$A_5 = 103993 = P,$ $B_5 = 33102 = 2 \cdot 3^3 \cdot 613,$
$A_6 = 104348 = 2^2 \cdot 19 \cdot 1373,$ $B_6 = 33215 = 5 \cdot 7 \cdot 13 \cdot 73,$
$A_7 = 208341 = 3^2 \cdot 7 \cdot 3307,$ $B_7 = 66317 = 17 \cdot 47 \cdot 83,$
$A_8 = 312689 = 13 \cdot 67 \cdot 359,$ $B_8 = 99532 = 2^2 \cdot 149 \cdot 167,$
$A_9 = 833719 = P,$ $B_9 = 265381 = P,$
$A_{10} = 1146408 = 2^3 \cdot 3 \cdot 37 \cdot 1291,$ $B_{10} = 364913 = 101 \cdot 3613,$
$A_{11} = 4272943 = P,$ $B_{11} = 1360120 = 2^3 \cdot 5 \cdot 37 \cdot 919,$
$A_{12} = 5419351 = 7^2 \cdot 19 \cdot 5821,$ $B_{12} = 1725033 = 3 \cdot 307 \cdot 1873,$
$A_{13} = 80143857 = 3^3 \cdot 2968291,$ $B_{13} = 25510582 = 2 \cdot 31 \cdot 479 \cdot 859,$
$A_{14} = 165707065 = 5 \cdot 23 \cdot 239 \cdot 6029,$ $B_{14} = 52746197 = 7^3 \cdot 103 \cdot 1493,$
$A_{15} = 245850922 = 2 \cdot 29 \cdot 1009 \cdot 4201,$ $B_{15} = 78256779 = 3 \cdot 53 \cdot 577 \cdot 853,$
$A_{16} = 411557987 = P,$ $B_{16} = 131002976 = 2^5 \cdot 13 \cdot 29 \cdot 10859,$
$A_{17} = 1068966896 = 2^4 \cdot 89 \cdot 750679,$ $B_{17} = 340262731 = 41 \cdot 8299091,$
$A_{18} = 2549491779 = 3 \cdot 14081 \cdot 60353,$ $B_{18} = 811528438 = 2 \cdot 7 \cdot 71 \cdot 816427,$
$A_{19} = 6167950454 = 2 \cdot 67 \cdot 151 \cdot 304831,$ $B_{19} = 1963319607 = 3^3 \cdot 421 \cdot 172721,$
$A_{20} = 14885392687 = 11 \cdot 29 \cdot 373 \cdot 125101,$ $B_{20} = 4738167652 = 2^2 \cdot 109 \cdot 691 \cdot 15727.$

[1]) BARLOW's Tables of squares, cubes, square roots, cube roots and reciprocals (London 1930).

[2]) Sphinx, Revue mensuelle des questions récréatives, Bruxelles, 1938, S. 84.

Eine besondere Gesetzmäßigkeit in den Faktoren ist nicht zu erkennen. Anders ist es bei der Kettenbruchentwicklung der Zahl $e$, wo sich wenigstens für die kleinen Faktoren eine bestimmte Regelmäßigkeit ergibt[1]).

### 4. *Rechenmaschine*

Bei vielstelligen Zahlen kann es sich empfehlen, nicht die Division von links, sondern diejenige von rechts zu verschärfen. Dies kann mit Hilfe einer Rechenmaschine geschehen. Die Methode bleibt im Prinzip dieselbe, nur die Anordnung wird etwas geändert. Als Beispiel seien primitive Faktoren[2]) von Zahlen der Form $a^m \pm b^m$ oder speziell $a^m + 1$ gesucht; diese müssen die Form $km + 1$ bzw. $2km + 1$ besitzen. Ist zum Beispiel $m = 25$, so kommen für die Faktoren nur die Endziffern 01 und 51 in Frage.

Es sei die Zahl $n = 5938669651$ als Teiler der Zahl $9^{25} - 5^{25}$ gegeben. Man stellt sich zunächst die folgende Tabelle her, welche zu gegebenen Faktoren $p$ die sechsstelligen Endungen von $q$ angibt und aus einer Ober-, zwei Haupt- und zwei Unterzeilen besteht:

$n = 5938669651; \quad \sqrt{n} = 77062, \ldots$

| $d$ | $p$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 5449 | 01 | 669651 | 2145 | 7794 | 3643 | 9692 | 5941 | 2390 | 9039 | 5888 | 2937 |
| | | 349 | 5 | 7 | 9 | 1 | 3 | 5 | 7 | 9 | 1 |
| 3049 | 51 | 189607 | 4945 | 8194 | 1643 | 5292 | 9141 | 3190 | 7439 | 1888 | 6537 |
| | | 949 | 1 | 3 | 5 | 7 | 9 | 1 | 3 | 5 | 7 |

In der zweiten Kolonne stehen die Endziffern $p_2 p_1$, also 01 und 51, von $p$, oben in der Oberzeile die drittletzte Ziffer $p_3$ von $p$. Unter $p_3$ sind in den Hauptzeilen die zu $000 p_3 p_2 p_1$ gehörigen sechs Endziffern von $q$ angegeben, wobei aber die zwei letzten Ziffern $q_2 q_1$, hier also 51, bzw. 01, nur einmal (kursiv) unter 0 aufgeführt sind, da sie sich in den folgenden Kolonnen gleichbleiben. Es ist zum Beispiel $101 \cdot 214551 = 21669651$, was in den letzten sechs Stellen mit $n$ übereinstimmt. Die unter $p_3 = 0$ stehenden Zahlen findet man direkt durch Division von $n$ durch 01 bzw. 51 von rechts, die folgenden durch eine Progression zweiten Grades, deren erste Differenz $d$ ganz links in der ersten Kolonne angegeben ist. Wegen

$$(p + 100)(q + 100d) \equiv pq \pmod{10^6}$$

ist

$$-d(p + 100) \equiv q \pmod{10^4};$$

man findet also $d$, indem man die zu $p$ gehörige Zahl $q$ auf vier Stellen von rechts durch $p + 100$ dividiert und die Ergänzung zu 10000 bildet. Wird $p$ nochmals um 100 vergrößert, so findet man mit

$$-(d + 100e)(p + 200) \equiv q + 100d \pmod{10^4},$$

das heißt

$$ep \equiv -2d \pmod{100}$$

die zweite Differenz $e$ in Einheiten der viertletzten Stelle, indem man $-2d \pmod{100}$

[1]) Siehe El. Math., Bd. I, Heft 5, S. 93.

[2]) Vgl. Fußnote [1]), S. 5.

von rechts auf zwei Stellen durch $p$ dividiert. Wegen $-dp \equiv q \pmod{100}$ gilt auch

$$ep^2 \equiv 2q \pmod{100};$$

man kann also $e$ auch finden, indem man $2q$ auf zwei Stellen von rechts durch die beiden letzten Stellen von $p^2$ dividiert. Übrigens lassen sich alle Differenzen auch empirisch bestimmen oder kontrollieren, indem man weitere Zahlen der Tabelle durch Division von rechts direkt ausrechnet. Im betrachteten Beispiel wird $e = 2$. Damit lassen sich, besonders bei Verwendung einer Rechenmaschine, die weiteren Zahlen der Hauptzeilen sehr leicht anschreiben. Geht man dabei noch um einen Schritt über $p_3 = 9$ hinaus, so findet man den zu $p + 1000$ gehörigen Wert $q + 1000\,\delta$ und notiert sich in der Unterzeile die dreistellige Zahl $\delta$. Die beiden letzten Ziffern von $\delta$ müssen mit denen von $d$ übereinstimmen, sie bleiben durch die ganze Zeile dieselben und werden deshalb nicht wiederholt. Die erste Ziffer von $\delta$ ergibt eine arithmetische Progression, deren Differenz mit der letzten Ziffer von $e$ übereinstimmt.

Nachdem so die Tabelle hergestellt ist, lassen sich zu beliebigen Werten von $p$ die sechs Endstellen von $q$ leicht finden, denn wenn $p$ fortgesetzt um 1000 vermehrt wird, bleibt die Differenz $\delta$ konstant. Man entnimmt also der zu $p_2p_1$ gehörenden Hauptzeile die unter $p_3$ stehende Zahl, ergänzt durch die Endziffern $q_2q_1$, und addiert dazu das $p_6p_5p_4000$-fache der aus der Unterzeile zu entnehmenden Zahl $\delta$. Das Resultat kann dann mit dem durch Division von links erhaltenen verglichen werden, wozu im allgemeinen der Rechenschieber genügen wird.

Um jetzt mit Hilfe der Rechenmaschine die Faktoren der gegebenen Zahl zu finden, stellt man im Beispiel zunächst die Zahl 669651 im Resultatwerk ein, sodann im Einstellwerk die Zahl $349000 = 1000\,\delta$, die mit jeder Kurbeldrehung im Resultatwerk addiert wird. Gleichzeitig verfolgt man auf dem Rechenschieber die den Zahlen $p = 1001, 2001, 3001$ usw. gegenüberstehenden Zahlen $q$ und sieht zu, ob ihre sechste, eventuell fünfte, vierte usw. Stelle von rechts mit den entsprechenden Zahlen der Rechenmaschine übereinstimmen. Wenn dies nicht der Fall ist, geht man weiter, andernfalls kann man die Faktoren wie früher genauer untersuchen. Die Anzahl der Kurbeldrehungen (und damit die Zahl $p$) ist dem Zählwerk zu entnehmen, sofern dieses mit Zehnerübertragung versehen ist, andernfalls kann man bei einer vielstelligen Maschine in hinreichendem Abstand links von der Zahl $\delta$ im Einstellwerk noch eine einzelne 1 einstellen.

Wenn man so unterhalb $\sqrt{n}$, im Beispiel also unter 77062, keinen Faktor der Gestalt $p_5p_4001$ gefunden hat, geht man zum nächsten Feld der Tabelle, addiert also zu 214551 die Vielfachen von 549000 und vergleicht mit den Zahlen $q$ des Rechenschiebers, welche den Zahlen $p = 101, 1101, 2101, 3101$ usw. gegenüberstehen. So kann man fortfahren und findet schließlich im letzten Feld der Tabelle die Zerlegung $5938669651 = 70951 \cdot 83701$.

Praktisch wird man allerdings dieses Resultat schon früher erhalten. Man findet schon bei der Endung 701 von $p$, daß die «verdächtigen» Werte von $q$ ziemlich regelmäßig aufeinanderfolgen und wird diese Erscheinung über $\sqrt{n}$ hinaus verfolgen. So kommt man schon in der ersten Zeile zu dem Produkt $83701 \cdot 70951$. Es empfiehlt sich auch sonst, bei einer passenden Hälfte der Zahlen, hier bei den Endungen 01 von $p$, mit den Versuchen ein bestimmtes Stück über $\sqrt{n}$ hinauszugehen, man kann

dann bei der andern Hälfte, das heißt hier bei den Endungen 01 von $q$, entsprechend früher aufhören. Sobald nämlich $p$ größer wird als $n:100000$, so ist $q$ höchstens fünfstellig, also die Ziffer $q_6$ gleich 0. Dies ist auf der Rechenmaschine leicht zu prüfen, und je nach der Zahl $\delta$ ergeben sich empirisch Regelmäßigkeiten, die man ausnützen wird, um viele nicht in Betracht kommende Zwischenwerte zu überspringen.

Unter Umständen kann sich eine Zerlegung schon sehr früh ergeben; bei der unten aufgeführten Zahl 2161599151 findet sie sich an Hand der zugehörigen Tabelle nach den ersten neun Kurbeldrehungen; wenn eine Zahl jedoch Primzahl ist, muß die ganze Tabelle durchgenommen werden.

Anstatt sechs kann man auch acht Endstellen berücksichtigen und eine entsprechend größere Tabelle anlegen, die ganz nach demselben Prinzip aufgebaut ist. Als Beispiel werde die vierzehnstellige Zahl 10227209596001, ein Faktor der Zahl $20^{35}-1$, betrachtet. Die Faktoren müssen wieder auf 01 oder 51 enden, die achtstellige Tabelle enthält jetzt 20 Haupt- und Unterzeilen. Die erste und fünfte seien hier angegeben:

$n = 10227209596001; \quad \sqrt{n} = 3198000, \ldots$

| $d$ | $p$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 04999 | 001 | 09596*001* | 14595 | 21594 | 30593 | 41592 | 54591 | 69590 | 86589 | 05588 | 26587 |
| | | *3999* | 5 | 7 | 9 | 1 | 3 | 5 | 7 | 9 | 1 |
| 85399 | 201 | 22435*801* | 07834 | 95233 | 84632 | 76031 | 69430 | 64829 | 62228 | 61627 | 63026 |
| | | *4399* | 6 | 8 | 0 | 2 | 4 | 6 | 8 | 0 | 2 |

Prüft man die Faktoren $p$ jeweils nur bis zu $\sqrt{n}$, also bis zu 3198000, so ergibt sich hier die Zerlegung erst sehr spät. Es ist wiederum von Vorteil, bei einem Teil der Zahlen über $\sqrt{n}$ hinaus, etwa bis zu 10300000 zu gehen, man braucht dann die korrespondierenden Zahlen (mit vertauschten Endungen von $p$ und $q$) nur bis 1000000 durchzunehmen. In diesem Falle findet man die Zerlegung $7466201 \cdot 1369801$ schon im «Feld 6» der fünften Zeile. Ergänzt man die dort stehende Zahl 64829 durch die im «Feld 0» angegebenen Endstellen 801 zu 64829801 und addiert dazu das 746-fache der aus der Unterzeile zu entnehmenden Zahl 63990000, so erhält man eine Zahl mit den Endstellen 01369801, welche die vollständige Zahl $q$ ergeben. Die ersten Stellen stimmen mit den auf dem Rechenschieber (oder der Rechenwalze) abzulesenden überein; auch die Neuner- und Elferprobe stimmt, man kann das Resultat noch durch direktes Ausrechnen verifizieren.

Ehe man zu diesem Resultat gelangt, findet man ebenfalls in der fünften Zeile ein verdächtiges Produkt $2860201 \cdot 3575801$, bei dem nicht nur der Rechenschieber, sondern auch die Rechenwalze noch gute Übereinstimmung zeigt, bei dem aber die Neunerprobe nicht stimmt. Ausmultipliziert ergibt sich die Zahl 10227509596001, die sich von der gegebenen nur um 3 Einheiten der sechsten Stelle von links, also der neunten Stelle von rechts, unterscheidet; die acht letzten Stellen müssen ja nach Konstruktion richtig sein. Man wird solche Produkte zur Kontrolle notieren und ausrechnen.

Wenn man für die Zahl $n$ eine Zerlegung gefunden hat, so ist das Resultat durch die direkte Ausrechnung gesichert; es ist höchstens noch zu untersuchen, ob die

gefundenen Faktoren nicht weiter zerlegbar sind. Hat man jedoch keinen Faktor gefunden, so hat man keine direkte Probe, ob die Zahl tatsächlich Primzahl ist; man müßte, um das Resultat zu prüfen, das ganze Durchsuchen wiederholen. Es ist jedoch zu bemerken, daß das angegebene Verfahren gegen Fehler ziemlich unempfindlich ist. Systematische Fehler lassen sich durch passende Proben vermeiden, und Einzelfehler können sich nur dann auswirken, wenn die Zahl $n$ zerlegbar ist und der Fehler gerade das Feld betrifft, in welchem sich ein Faktor von $n$ ergeben würde. Die verdächtigen Produkte machen sich meistens so deutlich bemerkbar, daß das «Übersehen» einer Lösung kaum eintreten wird. Höchstens bei alleiniger Verwendung des Rechenschiebers oder der Rechenwalze für relativ große Zahlen und bei sehr ungleichen Faktoren ist die Gefahr etwas größer. Bei einiger Sorgfalt kann man sich aber auch in dem Falle, wo keine Zerlegung gefunden wurde, auf das Resultat verlassen.

Wenn es auch andere Methoden gibt, die in manchen Fällen schneller zum Ziel führen oder noch größere Zahlen zu behandeln gestatten, so hat die hier dargelegte doch den Vorteil, ohne besondere Vorkenntnisse oder schwierigere Entwicklungen auf beliebige, nicht zu große Zahlen anwendbar zu sein.

Zum Schluß seien einige Resultate zusammengestellt, die in der angegebenen Weise gefunden wurden. Die Zerlegung der Zahlen $a^{20}+1$ wird dadurch bis zu $a=10$, die der Zahlen $a^{10}+1$ bis zu $a=44$, und wenn $a=2x^2$, bis zu $x=24$, wenn $a=10x^2$, bis zu $x=8$ vollständig[1]). Die Zahlen der Form $(a^{25}-b^{25}):(a^5-b^5)$ mit $a=x^2$, $b=5y^2$ lassen sich algebraisch in $L\cdot M$ zerlegen, wobei mit $X=a^5$, $Y=b^5$, $Q=(X^2+3XY+Y^2)$, $R=\sqrt{5XY}\,(X+Y)$, $L=Q-R$, $M=Q+R$ wird. Im Falle $a=16$, $b=5$ sind die Faktoren 251 von $L$ und 151 von $M$, im Falle $a=1$, $b=20$ die Zerlegung $151\cdot1451\cdot46794901$ von $M$ schon bekannt[2]).

Als Primzahlen ergaben sich:

| | | |
|---|---|---|
| 810221830361, | Teiler von | $7^{20}+1$, |
| 208518605101, | » » | $26^{10}+1$, |
| 1784250435661, | » » | $34^{10}+1$, |
| 23674060981, | » » | $578^{10}+1$, |
| 1308636140501, | » » | $1058^{10}+1$, |
| 50150933101, | » » | $5^{25}+1$, |
| 3883402651, | » » | $16^{25}-5^{25}$ $(L:251)$, |
| 8238208751, | » » | $16^{25}-5^{25}$ $(M:151)$; |

als zusammengesetzt:

| | | |
|---|---|---|
| $190122908881 = 110321\cdot1723361$, | Teiler von | $640^{10}+1$, |
| $2161599151 = 9001\cdot240151$, | » » | $9^{25}-5^{25}$ $(L)$, |
| $5938669651 = 70951\cdot83701$, | » » | $9^{25}-5^{25}$ $(M)$, |
| $10227209596001 = 1369801\cdot7466201$, | » » | $20^{25}-1$ $(L)$. |

P. FINSLER, Zürich

---

[1]) KRAITCHIK, Recherches II, S. 89, 94, 95, 134–136, 145. Siehe auch Sphinx, 1937, S. 39.

[2]) CUNNINGHAM, Bin. Fact. II, S. 176.