Zur Faktorisierung der Fermat-Zahlen

Diplomarbeit in Mathematik

Fachbereich Mathematik und Informatik
Universität Bremen

Gutachter:
Prof. Dr. Jens Gamst
Prof. Dr. Wolfgang Fischer

vorg elegt von Ivka Curic

im Oktober 1998

Inhaltsverzeichnis

1 Einleitung

1.1 Vorwort

Die Zahlentheorie beschäftigt sich mit den Teilbarkeitseigenschaften ganzer und vor allem natürlicher Zahlen. Sie ist eines der ältesten Gebiete der Mathematik und im Laufe der Jahrtausende sind aus der Zahlentheorie sehr interessante Problemstellungen erwachsen, die sich positiv auf die gesamte Mathematik ausgewirkt haben.

Zur Entwicklung der Zahlentheorie haben viele große Mathematiker Beiträge geleistet, und auch heute ist dieser Zweig der Mathematik aufgrund seiner zahlreichen ungelösten Probleme für die mathematische Forschung von höchstem Interesse. Schon vor über 3000 Jahren erhielt die Zahlentheorie wesentliche Impulse von griechischen, indischen und chinesischen Gelehrten. Bereits im griechischen Altertum entstanden Mathematikbücher wie *Euklid*'s "Elemente" und *Diophant*'s "Arithmetika', die sich unter anderem auch mit der systematischen Behandlung ganzzahliger Fragestellungen befaßten. Mit dem ausgehenden Altertum schwand jedoch weitgehend das Interesse an der Mathematik insgesamt. Und wirklich starke, neue Impulse erhielt die Zahlentheorie erst wieder im 17. und 18. Jahrhundert, vor allem durch *Pierre de Fermat* (1601 bis 1665), welcher als "Vater der modernen Zahlentheorie" angesehen wird und durch *Leonhard Euler* (1707 bis 1783), welcher die Verbindung zwischen Analysis und Zahlentheorie schaffte.

In der Folgezeit wurden wesentliche Beiträge zur Zahlentheorie von dem großen deutschen Mathematiker *Carl Friedrich Gauß* (1777 bis 1855) geliefert, welcher die Zahlentheorie die "Königin der Mathematik" nannte (vgl. Scheid [24], Baker [2], Freud [9]).

Ein besonderes Interesse in der Zahlentheorie kommt den Primzahlen zu, also jenen natürlichen Zahlen größer als 1, die nur durch 1 und durch sich selbst teilbar sind. Die Folge der Primzahlen beginnt mit $2, 3, 5, 7, 11, 13, 17, \ldots$ Schon *Euklid* gibt in seinem Buch "Elemente der Mathematik" einen Beweis dafür an, daß die Folge der Primzahlen nicht abbricht, also daß es unendlich viele Primzahlen gibt (vgl. auch Bemerkung 1 auf Seite 6).

Wie viele Mathematiker vor und nach ihm, beschäftigte auch *Fermat* das

Problem der Primzahlen sehr. Er suchte nach Ausdrücken, die Primzahlen ergeben, sozusagen nach "Erzeugenden" von Primzahlen. Er äußerte die Behauptung, der Ausdruck

$$F_n = 2^{2^n} + 1 \qquad (n \in \mathbb{N})$$

sei eine solche "Erzeugende". Die Untersuchung genau dieser Ausdrücke ist das Thema meiner Arbeit.

Die Arbeit ist in 5 Kapitel gegliedert. Als erstes, d.h. noch in diesem Abschnitt, werden die grundlegenden Eigenschaften dieser Fermat-Zahlen diskutiert.

In Kapitel 2 geht es dann gleich zu den Primzahlkriterien über, denn schon bei der Einführung wird sich herausstellen, daß die Behauptung, *alle* Fermat-Zahlen F_n seien prim, falsch ist.

Die Kunst der Faktorisierung großer Zahlen, wie in diesem Fall der Fermat-Zahlen, war vor der Entwicklung moderner Computer nicht sehr fortgeschritten; erst mit der Verwendung von Computern haben die einzelnen Faktorisierungsalgorithmen ihren "praktischen Nutzen" erwiesen. In Kapitel 3 werden zunächst einige "klassische" Faktorisierungsmethoden kurz skizziert. Diese Methoden sind immer noch wichtig, da viele dieser Grundideen auch im Zusammenhang mit modernen Faktorisierungsmethoden verwendet werden.

Anschließend, in Kapitel 4, wird die Kettenbruchmethode bzw. der Faktorisierungsalgorithmus von *Morrison* & *Brillhart* als eine der ersten modernen Faktorisierungsmethoden detaillierter beschrieben, wobei vorher eine kurze Einführung in die Theorie der Kettenbrüche nötig ist.

In Kapitel 5 schließlich werden alle bekannten Primfaktoren der Fermat-Zahlen zusammengestellt.

1.2 Allgemeines über Fermat-Zahlen

Definition 1.2.1
Die Zahlen der Form

$$F_n = 2^{2^n} + 1 \qquad n = 0, 1, 2, \ldots$$

heißen Fermat-Zahlen.

Sie sind nach dem Französischen Mathematiker *Pierre de Fermat* benannt, der als erster Zahlen von solcher Form betrachtete.

Durch *F.M Mersenne* angeregt (vgl. Scharlau/Opolka [23]), begann *Fermat*, Anwalt und Parlamentsrat, etwa ab 1635 sich mit zahlentheoretischen

Fragen zu beschäftigen. Als erstes interessierte er sich für vollkommene (perfekte) Zahlen, "befreundete" Zahlen und ähnliche zahlentheoretische Spielereien. Aus diesem Zusammenhang dann entstand sein Interesse an dem Faktorisieren der Zahlen der Form $2^m \pm 1$.

Fermat wußte, daß

Lemma 1.2.2

Eine Zahl N der Form $N = 2^m + 1$ ist (höchstens) dann prim, falls m eine Zweierpotenz ist (falls also N eine sogenannte Fermat'sche Primzahl ist).

Beweis:

Wäre m keine Potenz von 2, so könnte man m als Produkt mit einem ungeraden Faktor $v > 1$ schreiben: $m = v \cdot w$ (w passend gewählt).

Dann aber gilt:

$$2^m + 1 = 2^{vw} + 1 = (2^w + 1)(1 - 2^w + 2^{2w} - \ldots + 2^{(v-1)w}) ,$$

was man durch Ausmultiplizieren leicht bestätigt.

Wegen $1 \leq w < m$ gilt: $1 < 2^w + 1 < 2^m + 1$, so daß die Zerlegung nichttrivial und damit $2^m + 1$ keine Primzahl ist. Daher muß m eine Potenz von 2 sein.

q.e.d.

Nun sprach *Fermat* 1640 in einem Brief an *Frencile de Bessy* die Vermutung aus, daß jede der Zahlen F_n eine Primzahl sei. Diese Vermutung wurde wenig später auch von *Mersenne* übernommen (vgl. Dickson[7], S. 375). *Fermat* gab aber zu, keinen Beweis für seine Behauptung zu besitzen.

Für $n \leq 4$ is die Behauptung in der Tat richtig, wie auch *Fermat* wußte:

$$\begin{aligned} F_0 &= 2 + 1 = 3, \\ F_1 &= 2^2 + 1 = 5, \\ F_2 &= 2^4 + 1 = 17, \\ F_3 &= 2^8 + 1 = 257, \\ F_4 &= 2^{16} + 1 = 65537 \end{aligned}$$

sind Primzahlen (vgl. Beispiel auf S. 14).

Während der Jahre 1729/30 (vgl. Dickson [7]) lenkte *C. Goldbach* in einer Korrespondenz mit *Euler* dessen Aufmerksamkeit auf *Fermats* erwähnte Vermutung. Diese wurde 1732 von *Euler* widerlegt. *Euler* zeigte nämlich, daß $F_5 = 4294967297$ zusammengesetzt (d.h. keine Primzahl) ist, genauer, daß F_5 von der Primzahl 641 geteilt wird (dazu mehr auf Seite 10f).

Die Folge der Fermat-Zahlen erhält man durch die Formel $F_{n+1} - 1 = (F_n - 1)^2$. Ihr Wachstum vollzieht sich also im Wesentlichen durch ständiges

Quadrieren, d.h. sie wächst sehr schnell. Bereits die Fermat-Zahl $F_5 = 2^{32}+1$ hat 10 Stellen, und z.B. F_{24} sogar über 5 Millionen Dezimalstellen.

Lemma 1.2.3

Alle Fermat-Zahlen sind paarweise zueinander teilerfremd.

Beweis:

Behauptung:

$$F_{m+1} - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_m \quad \text{für alle m} .$$

Dazu Induktion nach m:

$$m = 0 : \quad F_1 - 2 = F_0 \quad \text{bzw. } 5 - 2 = 3 .$$

Sei die Behauptung für $m = k$ bewiesen.
Dann

$$\begin{aligned} F_0 \cdot F_1 \cdot \ldots \cdot F_{k-1} \cdot F_k &= (F_k - 2) \cdot F_k \\ &= (2^{2^k} + 1 - 2) \cdot (2^{2^k} + 1) \\ &= (2^{2^k} - 1) \cdot (2^{2^k} + 1) \\ &= (2^{2^k})^2 - 1 = 2^{2^{k+1}} + 1 - 2 = F_{k+1} - 2. \end{aligned}$$

Daher, wenn $n < m$, dann $F_n | F_m - 2$. Wenn ein p existiert mit $p|F_n$ und $p|F_m$, dann auch $p|F_m - 2$, also auch $p|2$, woraus folgt, daß $p = 2$.
Da F_n ungerade für alle n ist, ist das ein Widerspruch zur Existenz eines solchen p.

q.e.d.

Bemerkung 1:

Aus der paarweisen Teilerfremdheit der Fermat-Zahlen zueinander kann man auf die Existenz von unendlich vielen Primzahlen schließen, denn jede Fermat-Zahl enthält Primfaktoren, die in den vorangehenden Fermat-Zahlen noch nicht vorgekommen sind. □

Bemerkung 2:

Die Fermat-Zahlen spielen z.B. auch in der Algebra eine gewisse Rolle, und zwar tauchen sie bei der Lösung des Konstruktionsproblems für das regelmäßige k-Eck durch *Gauß* auf. Nach *Gauß* gelingt die k-Teilung des Kreises allein mittels Zirkel und Lineal genau dann, wenn k die Form $2^{n_0} \cdot F_{n_1} \cdot \ldots \cdot F_{n_r}$ hat mit $n_0, \ldots, n_r \in \mathbb{N}$ und paarweise verschiedenen $n_1, \ldots, n_r$, so daß sämtliche Fermat-Zahlen $F_{n_1}, \ldots, F_{n_r}$ Primzahlen sind; dabei ist $r = 0$ erlaubt. □

2 Primzahlkriterien

2.1 Der "kleine" Fermat'sche Satz

> *"Dieser Satz, welcher sowohl wegen seiner Eleganz als auch wegen seines hervorragenden Nutzens höchst bemerkenswert ist, wird nach seinem Erfinder Fermat'sches Theorem genannt."*
>
> C.F. Gauß

Satz 2.1.1
Sei N eine Primzahl.
Dann gilt für jede nicht durch N teilbare ganze Zahl a:

$$a^{N-1} \equiv 1 \mod N .$$

Alternativ: Es gilt:

$$a^N \equiv a \bmod N$$

für jede Primzahl N und ganze Zahl a.

Bemerkung:
In einem Brief vom 18. Okt. 1640 an *Bessy* (vgl. Nikiforowski/Freiman [17] S. 121) teilte *Fermat* ohne Beweis dieses Resultat mit. Den ersten Beweis dieses Satzes gab *G.W. Leibniz*; *Euler* veröffentlichte dann ab 1736 einige Beweise für ihn.

Der Satz heißt nur wegen der Leichtigkeit seines Beweises der kleine Fermat'sche Satz. Als den großen Satz von *Fermat* bezeichnet man die Behauptung von *Fermat*, daß für $n \geq 3$ die Gleichung $x^n + y^n = z^n$ keine ganzzahligen Lösungen mit $x \cdot y \cdot z \neq 0$ besitzt. □

Der folgende elementare Beweis des kleinen Fermat'schen Satzes ist nur einer von vielen:

Beweis zu Satz 2.1.1
Per Induktion nach a:
Sei $a = 1$. Dann gilt: $1^N \equiv 1 \bmod N$.
Sei nun $a^N \equiv a \bmod N$ richtig für $a = m, m \geq 1$.
Dann gilt für $a = m + 1$:

$$\begin{aligned}(m+1)^N = m^N + 1 + \sum_{k=1}^{N-1} \binom{N}{k} m^{N-k} &\overset{(*)}{\equiv} m^N + 1 \bmod N \\ &\equiv m + 1 \bmod N .\end{aligned}$$

$(*)$: Man nutzt hier die Tatsache aus, daß $N \mid \binom{N}{k}$ für $1 \leq k \leq N-1$, denn: Wegen $k!\,\binom{N}{k} = N \cdot \ldots \cdot (N-k+1)$ geht N in $k!\,\binom{N}{k}$ auf, aber nicht in $k!$.

q.e.d.

Die Verallgemeinerung der Fermat'schen Kongruenz hat *Euler* entdeckt, die leicht mit den "Mitteln der Gruppentheorie" zu beweisen ist,bzw. da $\varphi(N)$ die Ordnung der multiplikativen Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$ ist, gilt:

Satz 2.1.2
Für natürliche Zahl $N \geq 2$ und ganze, zu N teilerfremde Zahl a gilt:

$$a^{\varphi(N)} \equiv 1 \bmod N\ .$$

(Dabei bezeichnet φ die Euler'sche Phi-Funktion, d.h. die Anzahl aller Zahlen $k \in \{0, 1, \ldots, N-1\}$, die zu N teilerfremd sind.)

□

Der kleine Fermat'sche Satz ist der Ausgangspunkt vieler guter und schneller Primzahltests. Die Fermat'sche Kongruenz ist eine notwendige Bedingung für N, um prim zu sein, und das ergibt ein

Kriterium für "Nicht-Primzahlen":
Ist $a^N \not\equiv a \bmod N$ für irgendeine ganze Zahl a, dann ist N keine Primzahl bzw. N ist zusammengesetzt.

Beispiel:
G.A. Paxon hat gezeigt, daß die Fermat-Zahl F_{13} wegen $3^{F_{13}} \not\equiv 3 \bmod F_{13}$ zusammengesetzt ist (vgl. Paxon [54]). □

Die Bedingung $a^{N-1} \equiv 1 \bmod N$ ist zwar, wie erwähnt, eine notwendige, aber keine hinreichende Bedingung dafür, daß N Primzahl ist, auch nicht, wenn man die trivialen Fälle $a = \pm 1$ ausschließt.

Beispiel:

$$2^{10} - 1 = 1023 = 3 \cdot 341$$

und daher

$$2^{340} \equiv 1 \bmod 341,$$

obwohl $341 = 11 \cdot 31$ keine Primzahl ist.
341 ist die kleinste Pseudoprimzahl. □

Definition 2.1.3

a) Eine ungerade zusammengesetzte Zahl N heißt Pseudoprimzahl, falls

$$a^{N-1} \equiv 1 \bmod N$$

für ein, zu N teilerfremdes, a.

b) Eine ungerade zusammengesetzte Zahl N heißt Carmichael-Zahl (oder absolute Pseudoprimzahl), wenn für alle zu N teilerfremden Zahlen a gilt:

$$a^{N-1} \equiv 1 \bmod N \ .$$

Nebenbemerkung:

Die unter b) definierten Zahlen sind nach *Robert D. Carmichael* benannt, der im Jahr 1909 eine Arbeit über diese Zahlen schrieb.

Die Vermutung, daß es unendlich viele Carmichael-Zahlen gibt, konnte erst 1994 bewiesen werden (vgl. Alford/Granville/Pomerance [28]). □

Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Die Carmichael-Zahlen sind diejenigen, die der Umkehrbarkeit des Satzes von *Fermat* am stärksten widersprechen.

Eine direkte Umkehrung des Satzes von *Fermat* ist also nicht möglich. Es wird sich aber im Abschnitt 2.3 dieses Kapitels herausstellen, daß die Kongruenz $a^{N-1} \equiv 1 \bmod N$ zusammen mit einigen zusätzlichen Bedingungen doch garantiert, daß N eine Primzahl ist.

2.2 Zur Form der Primfaktoren der Fermat-Zahlen

Wie schon erwähnt, behauptete *Fermat* und versuchte zu beweisen, daß alle Fermat-Zahlen prim sind. Diese Vermutung basiert anscheinend auf seiner Beobachtung, daß:

Lemma 2.2.1

Ist p ein Primteiler von $F_n = 2^{2^n} + 1$, dann gilt:

$$p \equiv 1 \bmod 2^{n+1} \ .$$

Ersten Beweis hierfür lieferte Euler. Heute würde man das z.B. so beweisen:

Beweis:

Ist p ein Primteiler von $F_n = 2^{2^n} + 1$, so gilt

$$2^{2^n} \equiv -1 \bmod p \qquad (*)$$

und daraus folgt $2^{2^{n+1}} \equiv 1 \bmod p$, d.h. die Ordnung von $(2 \bmod p)$ in der multiplikativen Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ ist ein Teiler von 2^{n+1}, und wegen $(*)$ ist die Ordnung von $(2 \bmod p)$ gleich 2^{n+1}. Da die Ordnung von $(\mathbb{Z}/p\mathbb{Z})^*$ gleich $p-1$ ist, folgt also:

$$2^{n+1} \mid (p-1)\ .$$

q.e.d.

Bemerkung:

Daß *Fermat* von dieser Bedingung wußte, wird dadurch deutlich, daß man zu diesem Schluß im Beweis auch über den kleinen Fermat'schen Satz kommt, welcher aus dem gleichen Jahr, 1640, stammte, wie die Vermutung, daß alle Fermat-Zahlen prim seien. Denn:

Aus $(*)$, d.h. $2^{2^n} \equiv -1 \bmod p$ und aus dem kleinen Fermat'schen Satz:

$$2^{p-1} \equiv 1 \bmod p$$

folgt die Behauptung, daß

$$2^{n+1} \mid (p-1).$$

□

Was die fünfte Fermat-Zahl $F_5 = 2^{32} + 1$ angeht, hätte *Fermat* also wissen müssen, daß jeder Primteiler p von F_5 von der Form $p \equiv 1 \bmod 2^6$ ist bzw., daß die Primteiler p unter den Zahlen

$$\{65, 129, 193, 257, 321, 385, 449, 513, 577, 641, \ldots\}$$

zu suchen sind. Aus dieser Zahlenfolge sind nur die Primzahlen

$$\{193, 257, 449, 577, 641, \ldots\}$$

von Interesse, wobei zusätzlich auch 257 uninteressant ist, da $F_3 = 257$, und wie wir nach Lemma 1.2.3 wissen, sind alle Fermat-Zahlen paarweise zueinander teilerfremd.

Es erscheint merkwürdig, daß *Fermat* in dieser Folge den Faktor 641 von F_5 nicht finden konnte, welcher nun nur die vierte Zahl in der Folge ist, die er als Primteiler hätte versuchen müssen.

1877 bewies *E. Lucas* mit Hilfe des zweiten Ergänzungssatzes zum quadratischen Reziprozitätsgesetz ein Ergebnis, welches die Form der möglichen Primfaktoren der Fermat-Zahlen noch weiter einschränkt:

Satz 2.2.2
Teilt eine Primzahl p die Fermat-Zahl F_n mit $n \geq 2$, so gilt:

$$p \equiv 1 \bmod 2^{n+2} .$$

Bevor ich diesen Satz beweise, formuliere ich die beiden Ergänzungssätze zum quadratischen Reziprozitätsgesetz als auch das quadratische Reziprozitätsgesetz, welche ich auch später mehrfach brauchen werde und deren Beweise man in jedem Lehrbuch über Zahlentheorie finden kann.

Vorbemerkung:
Für $ggT(a,p) = 1$ definiert man das Legendre-Symbol $(\frac{a}{p})$ durch

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & , \quad \text{falls } a \text{ quadratischer Rest mod } p \text{ ist} \\ -1 & , \quad \text{falls } a \text{ kein quadratischer Rest mod } p \text{ ist.} \end{cases}$$

(ggT: größter gemeinsamer Teiler.)

Satz 2.2.3
Sei p eine ungerade Primzahl.
Dann gilt:

a) $$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & , \quad \text{falls } p \equiv 1 \bmod 4, \\ -1 & , \quad \text{falls } p \equiv 3 \bmod 4. \end{cases}$$

b) $$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & , \quad \text{falls } p \equiv \pm 1 \bmod 8, \\ -1 & , \quad \text{falls } p \equiv \pm 3 \bmod 8. \end{cases}$$

wobei $\left(\frac{-1}{p}\right)$ bzw. $\left(\frac{2}{p}\right)$ das Legendre-Symbol bedeutet.

□

Satz 2.2.4 *(Quadratisches Reziprozitätsgesetz)*
Seien $p \neq q$ ungerade Primzahlen. Dann gilt:

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} .$$

Alternativ:
Es gilt

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \text{ falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4$$

und

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right), \text{ falls } p \equiv q \equiv 3 \bmod 4.$$

□

Beweis zum Satz 2.2.2:
Wir wissen bereits, daß $2^{n+1} \mid (p-1)$.
Wegen $n \geq 2$ ist $p \equiv 1 \bmod 8$. Nach Satz 2.2.3b) ist dann $(\frac{2}{p}) = 1$, d.h. es gilt $x^2 \equiv 2 \bmod p$ für eine geeignete ganze, zu p teilerfremde, Zahl x. Die letzte Kongruenz impliziert $x^{2^{n+2}} \equiv 2^{2^{n+1}} \equiv 1 \bmod p$.
Also

$$2^{n+2} | (p-1) \; .$$

q.e.d.

Es ist unklar, ob *Fermat* etwas über diese zweite strengere Bedingung $p \equiv 1 \bmod 2^{n+2}$ für Primteiler p von F_n wußte. Jedenfalls sind unter Berücksichtigung dieser strengeren Bedingung die Primteiler von F_5 unter $p \equiv 1 \bmod 2^7$ bzw. unter $\{129, 257, 641, \ldots\}$ zu suchen. Da $129 = 3 \cdot 43$ keine Primzahl ist und $257 = F_3$, sind sie uninteressant, d.h. hierbei ist 641 die erste "Test"-Zahl, bzw. nur eine Probedivision ist nötig. Man ist geneigt zu glauben, (vgl. Lenstra et al. [49]), daß *Fermat* nicht ernsthaft versucht hat, seine Vermutung numerisch zu verifizieren oder wenn doch, daß er dann dabei einen Rechenfehler beging.

Beispiel:
Ich will einen Primfaktor p von $F_{12} = 2^{4096} + 1$ suchen (vgl. Scheid [25], S. 212). Nach Satz 2.2.2 gilt $p \equiv 1 \bmod 2^{14}$.
Für $p_k = 2^{14} \cdot k + 1$ gilt:

(i) $p_4 = 2^{14} \cdot 4 + 1 = 2^{16} + 1 = F_4$, wegen $ggT(F_4, F_{12}) = 1$ (vgl. Lemma 1.2.3) kommt p_4 nicht als Primteiler von F_{12} in Frage.

(ii) Wegen $2^{14} \equiv 1 \bmod 3$ ist $p_k \equiv k + 1 \bmod 3$ und daher $3 | p_k$ für $k \equiv 2 \bmod 3$; es entfallen also die Zahlen $p_2, p_5, p_8, p_{11}, \ldots$.

(iii) Wegen $2^{14} \equiv 4 \bmod 5$ ist $p_k \equiv 4k + 1 \bmod 5$ und daher $5 | p_k$ für $k \equiv 1 \bmod 5$; es entfallen also die Zahlen $p_1, p_6, p_{11}, p_{16}, \ldots$.

(iv) Wegen $2^{14} \equiv 4 \bmod 7$ ist $p_k \equiv 4k + 1 \bmod 7$ und daher $7 | p_k$ für $k \equiv 2 \bmod 7$; es entfallen also die Zahlen $p_2, p_9, p_{16}, \ldots$.

(v) Wegen $2^{14} \equiv 5 \bmod 11$ ist $p_k \equiv 5k+1 \bmod 11$ und daher $11|p_k$ für $k \equiv 2 \bmod 11$; es entfallen also die Zahlen $p_2, p_{13}, p_{24}, \ldots$.

(vi) Wegen $2^{14} \equiv 4 \bmod 13$ ist $p_k \equiv 4k+1 \bmod 13$ und daher $13|p_k$ für $k \equiv 3 \bmod 13$; es entfallen also die Zahlen $p_3, p_{16}, p_{29}, \ldots$.

Die kleinste bisher verbliebene Zahl ist

$$p_7 = 2^{14} \cdot 7 + 1 = 114698 \ .$$

Man kann zeigen, daß tatsächlich p_7 ein Teiler von F_{12} ist (vgl. die Tabelle 2 in Kapitel 5). □

2.3 Zur Umkehrung des Satzes von Fermat

Wie bereits festgestellt wurde, ist eine direkte Umkehrung des Satzes von *Fermat* nicht möglich; es sind zusätzliche Bedingungen notwendig, um aus dem kleinen Fermat'schen Satz ein Primzahlkriterium zu schaffen.

Der folgende Satz ist ein Primzahlkriterium, welcher 1891 von *Lucas* angegeben und 1927 von *D.H. Lehmer* für praktische Zwecke etwas verbessert wurde:

Satz 2.3.1

Sei $N > 1$ gegeben.
Es existiere eine ganze Zahl $a > 1$, so daß

(i) $a^{N-1} \equiv 1 \bmod N$

(ii) $a^{(N-1)/p} \not\equiv 1 \bmod N$ für jeden Primteiler p von $(N-1)$.

Dann ist N prim.

In diesem Fall ist a eine Primitivwurzel modulo N, d.h. a erzeugt die multiplikative Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$.

Ursprünglich hate *Lucas* gefordert, daß die zweite Kongruenz für alle Teiler von $(N-1)$, sowohl prim als auch zusammengesetzt, erfüllt sein soll.

Beweis:

Nach Bedingung (i) teilt die Ordnung r von $(a \bmod N)$ die Zahl $(N-1)$. Also

$$N - 1 = k \cdot r, \qquad k \geq 1 \ .$$

Nun sei $k > 1$.

Sei weiter p ein Primteiler von k. Dann

$$p \mid (N-1)$$

und

$$a^{(N-1)/p} = (a^r)^{k/p} \equiv 1^{k/p} = 1 \bmod N \; .$$

Das ist ein Widerspruch zu der zweiten Bedingung und damit muß $k = 1$ sein.
Also $N - 1 = r$. Da $r \leq \varphi(N) \leq N - 1$, so ist $\varphi(N) = N - 1$. Daraus folgt die Behauptung.

q.e.d.

Das Kriterium des obigen Satzes wird auch $(p-1)-$Primzahltest genannt. Der Grund hierfür ist zugleich auch der Nachteil des Kriteriums, denn um für eine Zahl N zu beweisen, daß sie eine Primzahl ist, muß $(N-1)$ in Primfaktoren zerlegt werden, was für große Zahlen manchmal praktisch unmöglich ist. Für gewisse Spezialfälle, wie hier Fermat-Zahlen bietet sich der $(p-1)-$Primzahltest aber gerade an, da $F_n - 1 = 2^{2^n}$.

Beispiel:
Ich will zeigen, daß die vierte Fermat-Zahl $F_4 = 2^{2^4} + 1$ eine Primzahl ist. Dazu genügt es, ein a mit $a^{F_4-1} = a^{2^{16}} \equiv 1 \bmod F_4$ und $a^{(F_4-1)/2} = a^{2^{15}} \not\equiv 1 \bmod F_4$ zu finden. Die folgende Rechnung zeigt, daß man $a = 3$ wählen kann, d.h. 3 ist eine Primitivwurzel mod F_4.

$$F_4 = 2^{16} + 1 = 65537$$

Sukzessives Quadrieren mod F_4 ergibt:

i	0	1	2	3	4	5	6	7	8	9
$3^{2^i} \bmod F_4$	3	9	81	6561	54449	61869	19139	15029	282	13987

$$\begin{aligned}
3^{2^{10}} &= 3^{1024} \equiv 8224 = 8192 + 32 = 2^{13} + 2^5 \\
3^{2^{11}} &= 3^{2048} \equiv 2^{26} + 2^{19} + 2^{10} \equiv -2^{10} - 2^3 + 2^{10} \equiv -8 \\
3^{2^{12}} &= 3^{4096} \equiv 2^6 \\
3^{2^{13}} &= 3^{8192} \equiv 2^{12} \\
3^{2^{14}} &= 3^{16384} \equiv 2^{24} \equiv -2^8 \\
3^{2^{15}} &= 3^{32768} \equiv 2^{16} \equiv -1 \bmod F_4 \quad (!) \\
3^{2^{16}} &= 3^{65536} \equiv 1 \bmod F_4 \quad (!)
\end{aligned}$$

(vgl. hierzu auch den Satz 2.4.3 von *Pepin*). □

Allgemein gesehen ist ein weiterer Nachteil des $(p-1)$-Primzahltests das Unwissen, welche Basis a man wählen soll, so daß man in der Praxis einfach der Reihe nach die Zahlen $a \geq 2$, außer den Quadratzahlen, probieren muß. Falls für irgendeinen Primfaktor von $N-1$ die Bedingung (ii) des obigen Primzahlkriteriums nicht erfüllt ist, ist dann entweder N nicht prim oder a ist keine Primitivwurzel modulo N. Wenn man "zuversichtlich" gegenüber dem Primzahlsein von N ist, so probiert man weitere a aus und hofft auf gutes Glück, d.h. eine Primitivwurzel modulo N zu finden.

Das obige Kriterium wurde von *J. Brillhart*, *D.H. Lehmer* und *J.L. Selfridge* weiter verfeinert, so daß es nun nicht mehr nötig ist, eine Primitivwurzel modulo N zu finden, um zu beweisen, daß N prim ist:

Satz 2.3.2

Sei $N > 1$ gegeben.

Für jeden Primteiler p_i von $(N-1)$ existiere eine ganze Zahl a_i, so daß

(i) $a_i^{(N-1)} \equiv 1 \bmod N$

(ii) $a_i^{(N-1)/p_i} \not\equiv 1 \bmod N$

Dann ist N prim.

Beweis:

Sei $N-1 = p_1^{e_1} \cdot p_1^{e_2} \cdots p_r^{e_r}$ gegeben, und man habe a_i mit den geforderten Eigenschaften gefunden. Weiter sei $\mathrm{Ord}(a_i)$ die Ordnung von a_i mod N. Dann gilt für jedes i:

$$\mathrm{Ord}(a_i)|(N-1), \text{ aber } \mathrm{Ord}(a_i) \nmid (N-1)/p_i \ .$$

Daraus folgt

$$p_i^{e_i} | \ \mathrm{Ord}(a_i) \ .$$

Da $a^{\varphi(N)} \equiv 1 \bmod N$, so gilt: Ord $(a_i)|\varphi(N)$ und damit auch $p_i^{e_i}|\varphi(N)$. Da das für alle i richtig ist, muß gelten:

$$(N-1)|\varphi(N) \ .$$

Mit $\varphi(N) \leq (N-1)$ folgt $\varphi(N) = N-1$, und damit ist N prim.

q.e.d.

Nachteil des Kriteriums aus diesem Satz ist wieder die Primfaktorzerlegung von $(N-1)$, die oft nicht bekannt ist. Um das zu vermeiden und damit den Primzahltest effizienter zu machen, gibt es Kriterien, wo nur eine Teilzerlegung von $(N-1)$ gefordert wird. Das Grundergebnis hierfür bewies *H.C. Pocklington* 1916:

Satz 2.3.3

Sei $N-1 = q^n \cdot R$ mit q prim, $n \geq 1$ und $q \nmid R$. Es existiere eine ganze Zahl $a > 1$, so daß:

(i) $a^{(N-1)} \equiv 1 \bmod N$

(ii) $ggT(a^{(N-1)/q} - 1, N) = 1$.

Dann hat jeder Primteiler von N die Form:

$$m\, q^n + 1 \quad \text{mit} \quad m \geq 1 \, .$$

Beweis:

Sei p ein Primteiler von N und sei e die Ordnung von a mod p. Dann gilt: $e|(p-1)$ und $e|(N-1)$ nach (i). Da $p|N$, so gilt nach Bedingung (ii): $e \not| (N-1)/q$.

Daraus folgt, daß $q \nmid (N-1)/e$ (denn wäre $q|\frac{N-1}{e}$, so gälte $N-1 = e \cdot q \cdot f$, also $e|\frac{N-1}{q}$). Da aber $q^n|(N-1)$, so folgt: $q^n|e$ und damit auch $q^n|(p-1)$.

q.e.d.

Bemerkung:

Der Satz in der obigen Form ist eher eine Aussage über die Primfaktoren als ein Primzahltest.

Wenn man jedoch voraussetzt, daß q^n "groß genug" ist, z.B. $q^n > \sqrt{N}$, so folgt aus (i) und (ii), daß N prim ist; denn für jeden Primteiler p von N gilt dann: $q^n|(p-1)$ nach dem obigen Argument und damit $p > \sqrt{N}$, was nur sein kann, wenn N selbst prim ist. □

Der folgende Satz von *Lehmer* aus dem Jahr 1928 ist nur eine Verfeinerung des Satzes von *Pocklington*:

Satz 2.3.4

Sei $N-1 = F \cdot R$ mit $ggT(F, R) = 1$ und die Primfaktorzerlegung von F sei $F = p_1^{e_i} \cdot P_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$. Es existiere für jedes $i = 1, \ldots, r$ ein a_i so daß:

(i) $a_i^{(N-1)} \equiv 1 \bmod N$

(ii) $ggT(a_i^{(N-1)/p_i} - 1, N) = 1$.

Dann hat jeder Primteiler von N die Form $mF+1$ mit $m \geq 1$. Falls $F > \sqrt{N}$, dann ist N prim.

Beweis:

Sei p irgendein Primteiler von N. Für jedes $i = 1, \ldots, r$ sei b_i die Ordnung von a_i mod p. Dann: $b_i|(p-1)$ für jedes i. Da die Bedingung (i) impliziert:

$$a_i^{N-1} \equiv 1 \bmod p, \qquad \text{so ist} \qquad b_i|(N-1) \qquad \text{für alle } i\ .$$

Da auf der anderen Seite gilt:

$$a_i^{(N-1)/p_i} \not\equiv 1 \bmod p, \quad \text{so folgt} \quad b_i \nmid (N-1)/p_i\ .$$

Damit $p_i^{e_i}|b_i$ und auch $p_i^{e_i}|(p-1)$. Da das für alle i gilt, folgt: $F|(p-1)$. Damit gilt für alle Primteiler p von $N : p > F$. Falls nun $F > \sqrt{N}$ sein soll, so muß N prim sein.

q.e.d.

Bemerkung:

Neben diesen Primzahlkriterien, die Primfaktorzerlegung von $(p-1)$ voraussetzen, gibt es auch Primzahlkriterien, die Primfaktorzerlegung von $(p+1)$ voraussetzen, die aber ungeeignet für Fermat-Zahlen sind. Das Hilfsmittel zu diesen $(p+1)$-Primzahlkriterien sind sog. Lucas-Folgen (vgl. z.B. Forster [8]). □

2.4 Zu den Faktoren von Fermat-Zahlen

Wie schon gezeigt wurde, fand *Euler* einen Teiler der fünften Fermat-Zahl und zeigte damit, daß F_5 nicht prim ist. Daß auch weitere Fermat-Zahlen nicht prim sind, konnte man zeigen, indem man auch explizit einen Faktor fand. Dazu nützte der Satz 2.2.2 von *Lucas*.

Eine spezielle Suchmethode nach Faktoren der Form $p = k \cdot 2^m + 1$ (mit k ungerade und $m > 0$) von Fermat-Zahlen F_n fängt nicht damit an, daß man F_n festhält und nach p sucht (das wird das Thema der nächsten beiden Kapitel sein), sondern umgekehrt, daß man p fixiert und nach n mit $F_n \equiv 0$ mod p sucht. Dazu gibt es zwei Möglichkeiten:

a) Probedivision:
Für ein festes m sucht man nach k mit $(k \cdot 2^m + 1)|F_n, n \leq m-2$. Das überprüft man für alle k kleiner als eine vorgegebene Grenze K. Bei der Untersuchung, ob ein $d_k := k \cdot 2^m + 1$ ein F_n teilt, werden die Kongruenzen $2^{2^n} \equiv -1$ mod d_k wie folgt getestet:
Man beginnt mit dem Rest $r_i = 2^{2^i}$ für $i = 5$. Dann wird $r_{i+1} = r_i^2 - 1$ mod d_k berechnet. Das wird so lange wiederholt, bis irgendein i gefunden wird mit $r_i \equiv -1$ mod d_k oder $i = m-2$. Für jedes r_i mit

$r_i \equiv -1 \bmod d_k$ gilt dann: $d_k | F_i$
(vgl. Hallyburton/Brillhart [46]).

b) Auflisten der Primzahlen:
Für ein festes k listet man Primzahlen p der Form $p = k \cdot 2^m + 1$ für alle m kleiner als eine vorgegebene Grenze M auf und prüft anschließend, ob p ein F_n teilt, nur für $n \leq m-2$ (wegen des Satzes 2.2.2 von *Lucas*).

Wenn der Index n der zu untersuchenden Fermat-Zahlen F_n klein ist im Vergleich zu der oberen Grenze K für k, dann wird die erste Möglichkeit, also die "Probedivision", der zweiten vorgezogen.

Beispiel:
Mit der unter a) beschriebenen Methode auf einer Rechenmaschine fanden *J.C. Hallyburton* und *Brillhart* 1974 heraus, daß

$$(11613415 \cdot 2^{14} + 1) \mid F_{12} \quad \text{und} \quad (41365885 \cdot 2^{16} + 1) \mid F_{13} .$$

Die folgenden k-Intervalle wurden dabei "erfaßt":
Für $1 \leq k \leq K$, k ungerade, n Index von F_n:

n	K
8	1542455295
$9-13$	$16777215 = 2^{24}-1$
14	792008373
$15-22$	$16777215 = 2^{24}-1$

Die bis dahin bekannten Teiler (vgl. hierzu Tabelle 2 in Kapitel 5) wie z.B. der von *Western* 1903 auf ähnliche Weise entdeckte Teiler $(37 \cdot 2^{16} + 1)$ von F_9 wurden ausgelassen. □

Diese Methode wurde auch von *Suyama, Gostin, Baillie, Cormack* & *Williams*, u.a. erfolgreich benutzt. Allein *Gostin* entdeckte mit dieser Methode 52 Primfaktoren von verschiedenen Fermat-Zahlen, (vgl. hierzu Tab. 2 in Kapitel 5).

Auf der anderen Seite ist die zweite Möglichkeit, das "Auflisten der Primzahlen" der Form $k \cdot 2^m + 1$, attraktiver, wenn große obere Grenzen M für m vorgegeben sind.
Eine der ersten besonders umfangreichen Tabellen solcher Primzahlen wurde von *R.M. Robinson* 1958 präsentiert. Diese Tabelle enthielt alle Primzahlen der Form $k \cdot 2^m + 1$ für $k < 100$ und $m < 512$, und zusätzlich war die Schranke M für m in einigen Fällen vergrößert, und zwar:

$$\text{für } k = 1 \quad : \quad m < 8192$$

$$\begin{aligned} \text{für } k = 3 \quad &: \quad m < 1280 \\ \text{für } k = 5 \quad &: \quad m < 2005 \\ \text{für } k = 7 \quad &: \quad m < 1280 \ . \end{aligned}$$

Mit Hilfe dieser Tabelle und der unter b) beschriebenen Methode fand *Robinson* in den Jahren 1956 und 1957 insgesamt 20 Primfaktoren von verschiedenen Fermat-Zahlen, wie z.B. den Faktor $(21 \cdot 2^{41} + 1)$ von F_{39}, einige darunter in Zusammenarbeit mit *Selfridge* (vgl. Tab. 2 in Kapitel 5 und Robinson [62]).

Bevor man mit einer der beiden Suchmethoden beginnen konnte, wurden erst die Zahlen der Form $k \cdot 2^m + 1$ einem Primzahltest unterworfen, und zwar diente hierfür ein Kriterium, der 1878 von *F. Proth* angegeben, aber nicht bewiesen wurde:

Satz 2.4.1

Sei $N = k \cdot 2^m + 1$ gegeben mit $0 < k < 2^m$ und o.E. k ungerade. N ist prim genau dann, wenn eine Zahl a existiert mit

$$a^{\frac{(N-1)}{2}} \equiv -1 \bmod N \ .$$

Um diesen Satz zu beweisen, benutze ich ein wichtiges Kriterium von *Euler*:

Satz 2.4.2

Sei p eine ungerade Primzahl.
Dann gilt für jedes $a \in \mathbb{Z}$:

$$a^{\frac{(p-1)}{2}} \equiv (\frac{a}{p}) \bmod p \ .$$

Beweis zu Satz 2.4.2:

Sei g das erzeugende Element der zyklischen Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ von der Ordnung $p-1$. Dann ist

$$g^{(p-1)} \equiv 1 \bmod p \ .$$

Sei weiter $a = g^\alpha \bmod p$.

Ist a quadratischer Rest, dann ist α gerade, etwa $\alpha = 2\beta$ und dann gilt

$$a^{\frac{p-1}{2}} \equiv (g^{p-1})^\beta \equiv 1 \bmod p \ .$$

Ist a quadratischer Nichtrest, dann ist α ungerade, etwa $\alpha = 2\beta + 1$ und dann gilt:

$$a^{\frac{p-1}{2}} \equiv (g^{p-1})^\beta \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \bmod p \ .$$

q.e.d.

Beweis zu Satz 2.4.1:

$\Rightarrow$: Wähle a mit $\left(\frac{a}{N}\right) = -1$. Dann ist nach dem Satz 2.4.2 die Kongruenz erfüllt.

$\Leftarrow$: Sei $a^{\frac{N-1}{2}} \equiv -1 \bmod N$, wobei $N - 1 = k \cdot 2^m$ und $ggT(2^m, k) = 1$, da k ungerade.

Man hat dann

(i) $a^{N-1} \equiv 1 \bmod N$ und

(ii) $ggT(a^{\frac{N-1}{2}} - 1, N) = 1$.
Denn: Für jeden Primteiler $p|N$ und $p|a^{\frac{N-1}{2}} - 1$ gilt auch (nach Voraussetzung): $p|a^{\frac{N-1}{2}} + 1$ und damit folgt: $p|2$.
Da aber N ungerade ist, ist das ein Widerspruch.

Nach dem Satz 2.3.3 folgt nun aus (i) und (ii), daß für jeden Primteiler p von N gilt:

$$p \equiv 1 \bmod 2^m \ .$$

Also: $2^m | p - 1 \Rightarrow p > 2^m \Rightarrow p^2 > 2^{2m}$.
Da nach Voraussetzung: $2^m > k$, so gilt

$$2^{2m} \geq (k+1) \cdot 2^m \ .$$

Also: $p^2 > 2^{2m} \geq (k+1) \cdot 2^m > N$.
Damit: $p^2 > N$ für alle Primteiler $p|N$, also ist N prim.

q.e.d.

Ein Spezialfall des Satzes 2.4.1 von *Proth* wurde ein Jahr vorher, 1877, von *T. Pepin* bewiesen und wird in der folgenden Form für Primzahltests für Fermat-Zahlen gebraucht:

Satz 2.4.3
Die Zahl $F_n = 2^{2^n} + 1$ ist für $n \geq 1$ genau dann eine Primzahl, wenn

$$3^{\frac{F_n - 1}{2}} \equiv -1 \bmod F_n \ .$$

Beweis:

$\Leftarrow$: Sei $3^{\frac{F_n-1}{2}} \equiv -1 \bmod F_n$.
Dann ist nach dem Satz 2.4.1 von *Proth* F_n prim, (wobei $a = 3$ und $k = 1$).

$\Rightarrow$: Sei F_n eine Primzahl.
Dann gilt nach dem Satz 2.4.2 von *Euler*:

$$3^{\frac{F_n-1}{2}} \equiv (\frac{3}{F_n}) \bmod F_n \ .$$

Da $F_n \equiv 1 \bmod 4$, so gilt nach dem quadratischen Reziprozitätsgesetz (Satz 2.2.4):

$$(\frac{3}{F_n}) = (\frac{F_n}{3}) \ .$$

Nun gilt modulo 3

$$F_n \equiv (-1)^{2^n} + 1 \equiv 2 \bmod 3 \ ,$$

also $(\frac{F_n}{3}) = (\frac{2}{3}) = -1$ nach dem zweiten Ergänzungssatz (Satz 2.2.3*b)*).

q.e.d.

Notiz:
Pepin bemerkte, daß die obige Äquivalenz bei $n > 1$ auch mit Basis $a = 5$ bzw. $a = 10$ wegen $(\frac{5}{F_n}) = -1$ bzw. $(\frac{10}{F_n}) = -1$ richtig ist.
Denn: Da $F_n \equiv 1 \bmod 4$, so gilt

$$\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) \text{ und da } 2^n = 4 \cdot 2^{n-2},$$

so ist

$$F_n = 2^{2^n} + 1 \equiv (2^4)^{2^{n-2}} + 1 \equiv 2 \bmod 5$$

und

$$\left(\frac{2}{5}\right) = -1 \ .$$

Für Basis $a = 10$ geht es genauso, denn:

$$\begin{aligned} \left(\frac{2}{F_n}\right) &= (-1)^{\frac{F_n^2-1}{8}} = (-1)^{\frac{F_n-1}{4}\cdot\frac{F_n+1}{2}} = 1 \quad \text{und} \\ \left(\frac{10}{F_n}\right) &= \left(\frac{2}{F_n}\right) \cdot \left(\frac{5}{F_n}\right) = 1 \cdot (-1) = -1 \ . \end{aligned}$$

□

Bemerkung:
Wichtig ist vor allem:

$$F_n \text{ prim} \quad \Rightarrow \quad 3^{\frac{F_n-1}{2}} \equiv -1 \qquad \text{d.h.}$$

$$3^{\frac{F_n-1}{2}} \not\equiv -1 \quad \Rightarrow \quad F_n \text{ nicht prim.}$$

Man rechnet also $R_n = 3^{\frac{F_n-1}{2}} \bmod F_n$ aus, wobei Repräsentant von R_n in $\{0,1,\ldots,F_n-1\}$ ist, um zu zeigen ob F_n prim oder zusammengesetzt ist, d.h. ob $R_n = F_n - 1$ ist oder nicht.

Da $\frac{F_n-1}{2} = 2^{2^n-1}$, kann man $3^{\frac{F_n-1}{2}}$ durch (2^n-1)-maliges Quadrieren berechnen, d.h. der Rechenaufwand steigt exponentiell mit n.

Dieses Verfahren der Berechnung von Pepin-Rest R_n wurde benutzt, um zu zeigen, daß z.B. $F_7, F_8, F_{10}, F_{13}, F_{14}, F_{20}$ und F_{22} zusammengesetzt sind (vgl. Morehead [50], Morehead/Western [51], Robinson [59], Paxon [54], Selfridge/Hurwitz [65], Young/Buell [71], Crandall et al [40]).

F_{22} mit 1262612 Dezimalstellen ist die größte Zahl, die bisher dem Pepin'schen Test unterworfen wurde.

Gebenüber der Folgerung:

$$R_n \neq F_n - 1 \quad \Rightarrow \quad F_n \text{ ist zusammengesetzt,}$$

muß man aber etwas skeptisch sein, denn z.B. ein Rechenfehler würde zu einem falschen Rest führen, welcher dann die erwartete Annahme, die getestete Fermat-Zahl sei zusammengesetzt, bestätigen würde. Ob die Möglichkeit einer unkorrekten Implementierung des zugehörigen Algorithmus besteht, läßt sich mit sog. Selfridge- und Hurwitz-Resten (vgl. [65]) überprüfen; d.h. mit den von *Selfridge* und *Hurwitz* veröffentlichten Werten von R_n mod $2^{36}, 2^{36}-1, 2^{35}-1$ für F_7, F_8, F_{13} und F_{14} vergleicht man die durch das eigene Programm erzeugten Reste für die gleichen Fermat-Zahlen.

In der folgenden Tabelle, die von *Crandall et al* (vgl. [40]) angegeben wurde, sind die Selfridge- und Hurwitz-Reste für F_n, $5 \leq n \leq 22$ aufgeführt und also auch erweitert:

n	R_n mod $2^{35}-1$	R_n mod 2^{36}	R_n mod $2^{36}-1$
5	10324303	10324303	10324303
6	9190530327	8845352501	9017941414
7	5799525263	3909272836	44591026080
8	30627284506	46310188723	35403253324
9	28173182079	19661770102	54966870189
10	28022031617	36399120536	54182679152
11	3934743084	66666487080	44928212591
12	300454051	64546579219	3387502846
13	3434508623	52529728350	52864871946
14	15173315214	54038984522	1986493987
15	14110954287	7124011679	42435904961
16	173595305	24695037109	65390296136
17	14982977589	14726733277	2770550506
18	10874364700	46106404592	14070013587
19	6407009455	22254317980	58676148574
20	15265819636	16865158641	35626292569
21	30981963597	22442941248	300257643
22	12323430823	973723434	8733349067

Diese Selfridge-Hurwitz-Reste geben zwar nicht die vollständigen Pepin-Reste an, haben aber zwei Vorteile. Erstens sind diese Moduli relativ klein und daher sehr "handlich", d.h. zwischen den Teststellen schnell übertragbar. Zweitens bestätigt die Tatsache, daß hier für alle n mit $5 \leq n \leq 22$ der zweite Selfridge-Hurwitz-Rest nicht verschwindet ($\neq 0$), nochmals, daß $F_5, \ldots, F_{22}$ zusammengesetzt sind. □

Ein weiteres Kriterium für Primfaktoren von Fermat-Zahlen gibt der folgende

Satz 2.4.4

Eine Primzahl $N = k \cdot 2^m + 1$ ist ein Primteiler einer Fermat-Zahl F_n genau dann, wenn 2 ein k-ter Potenzrest modulo N ist.

Beweis:

Laut Definition ist 2 ein k-ter Potenzrest modulo N, falls die Kongruenz $x^k \equiv 2 \bmod N$ lösbar ist.

Wegen $ggT(2, N) = 1$ ist auch $ggT(x, N) = 1$. Dann gilt nach dem Fermat'schen bzw. Euler'schen Satz (Satz 2.1.1 bzw. 2.1.2):

$$(x^{N-1})^{k/k} \equiv 2^{\frac{N-1}{k}} \equiv 1 \bmod N \ .$$

Umgekehrt sei y Primitivwurzel mod N.
Dann existiert ein e mit $y^e \equiv 2 \bmod N$. Aus $2^{\frac{N-1}{k}} \equiv 1 \bmod N$ folgt dann:

$$y^{e \cdot \frac{N-1}{k}} \equiv 1 \bmod N \ .$$

Da y Primitivwurzel mod N ist, ist $N-1$ die Ordnung von ($y \bmod N$). Also gilt:

$$N - 1 \mid e \cdot \frac{N-1}{k}$$

und daraus folgt: $k \mid e$, also $e = k \cdot r$ für ein $r \in \mathbb{N}$. Damit:

$$2 \equiv y^{rk} \equiv (y^r)^k \bmod N,$$

d.h. $x^k \equiv 2 \bmod N$ ist lösbar mit $x \equiv y^r \bmod N$.
Also: 2 ist ein k-ter Potenzrest modulo N genau dann, wenn gilt:

$$2^{\frac{N-1}{k}} \equiv 1 \bmod N \qquad \text{bzw.} \qquad 2^{2^m} \equiv 1 \bmod N$$

(d.h. Ordnung von (2 mod N) ist von der Form 2^{n+1} mit $n + 1 \leq m$, d.h. $2^{2^n} \not\equiv 1 \bmod N$, aber $(2^{2^n})^2 \equiv 1 \bmod N$).
Also: genau dann, wenn gilt: $2^{2^n} \equiv -1 \bmod N$, da N prim ist.
Also: genau dann, wenn gilt: $N \mid F_n$. *q.e.d.*

Um zu entscheiden, ob N ein Faktor einer Fermat-Zahl ist, nützt dieses Kriterium gewöhnlich nicht viel, außer in einem Fall, der etwa 1907 von *J.C. Morehead* bewiesen wurde:

Satz 2.4.5

Eine Primzahl N der Form $N = 3 \cdot 2^m + 1$, wobei m gerade ist, kann nicht ein Faktor einer Fermat-Zahl F_n sein.

Beweis:

Eine Primzahl $N = 3 \cdot 2^m + 1$, also $N \equiv 1 \bmod 6$, ist nach dem Satz 2.4.4 genau dann ein Primteiler einer Fermat-Zahl F_n, wenn 2 ein 3-ter Potenzrest modulo N ist. Und es gilt

Satz:

Sei $p \equiv 1 \bmod 3$ eine Primzahl.
$x^3 \equiv 2 \bmod p$ ist genau dann lösbar, wenn es ganze Zahlen C und D gibt mit

$$p = C^2 + 27D^2 \ .$$

(Zum Beweis des Satzes vgl. z.B. Ireland/Rosen [13], S. 119.)

In unserem Fall ist $C = 1$ und $D = 2^{\frac{m}{2}}$, also nicht ein Vielfaches von 3. Also kann 2 kein kubischer Rest modulo N sein. *q.e.d.*

Ein Primzahltest für Kofaktoren der Fermat-Zahlen

Wenn bei einer Fermat-Zahl F_n ein Faktor gefunden wurde, sollte man dann, vor der Suche nach weiteren Faktoren dieser Zahl, den übriggebliebenen Kofaktor einem Primzahltest unterwerfen. Ein brauchbarer Primzahltest für Kofaktoren von Fermat-Zahlen wurde von *Suyama* (vgl. [68]) angegeben:

Satz 2.4.6

Sei $F_n = f \cdot G$,
wobei f ein "kleiner", nicht notwendig primer, Teiler und der Charakter von G unbekannt ist. Falls G prim ist, gilt

$$R_n^2 \equiv 3^{f-1} \bmod G\ ,$$

wobei $R_n = 3^{\frac{F_n-1}{2}} \bmod F_n$ definiert ist.

Beweis:

Sei G prim.
Dann gilt nach dem kleinen Fermat'schen Satz:

$$3^{G-1} \equiv 1 \bmod G\ .$$

Daraus folgt: $3^G \equiv 3 \bmod G$ bzw. $3^{\frac{F_n}{f}} \equiv 3 \bmod G$ also $3^{F_n} \equiv 3^f \bmod G$ und damit

$$3^{F_n-1} \equiv 3^{f-1} \bmod G\ .$$

Da $R_n = 3^{\frac{F_n-1}{2}} \bmod F_n$, ist also

$$R_n^2 = 3^{F_n-1} \bmod F_n$$

und damit

$$R_n^2 \equiv 3^{f-1} \bmod G\ .$$

q.e.d.

Wenn also die Kongruenz $R_n^2 \equiv 3^{f-1} \bmod G$ nicht gilt, so ist G zusammengesetzt.

Dieser Test hat den Vorteil, daß man die gegebenenfalls ausgerechneten Pepin-Reste verwenden kann. Außerdem ist der Exponent $(f-1)$ relativ klein, was positive Auswirkung auf die Rechenzeit hat.

2.5 Primzahlpotenzen als Faktoren von Fermat-Zahlen

Bevor man mit der Suche nach den Faktoren einer zusammengesetzten Zahl N beginnt, sollte man sicher sein, daß N keine Primzahlpotenz ist, was auch die meisten Faktorisierungsmethoden voraussetzen (vgl. Bernstein [31]). Was die Fermat-Zahlen angeht, so gilt:

Satz 2.5.1
Eine Fermat-Zahl F_n kann keine Primzahlpotenz sein.

Beweis:
Sei $F_n = 2^{2^n} + 1, n \geq 1$, eine Primzahlpotenz, d.h. $2^{2^n} + 1 = p^k$ mit $k > 1, p$ Primzahl.

Sei $k \geq 2$ gerade.

Dann gilt: $1 = p^{2\cdot\ell} - 2^{2\cdot m}$ mit $k = 2 \cdot \ell, \ell \geq 1$ und $m = 2^{n-1}$, d.h. man hat zwei positive Quadrate, die sich um 1 unterscheiden, was unmöglich ist. Also ein Widerspruch.

Sei nun $k \geq 3$ ungerade.

Aus $p^k - 1 = 2^{2\cdot m}$ mit $m = 2^{n-1}$ folgt dann
$p^k - 1 = (p-1)(1 + p + \ldots + p^{k-1}) = 4^m$. Da k ungerade ist, ist der Faktor $(1 + p + \ldots + p^{k-1}) > 1$ auch ungerade und damit $(1 + p + \ldots + p^{k-1}) \nmid 4^m$, d.h. ein Widerspruch.

q.e.d.

Nun zu der Frage, ob die einzelnen Faktoren von Fermat-Zahlen Primzahlpotenzen sein können. Dazu als nächstes der

Satz 2.5.2
Sei p ein Primteiler einer Fermat-Zahl F_n. p^2 ist ein Teiler von F_n genau dann, wenn p der sog. Wieferich-Kongruenz $2^{p-1} \equiv 1 \bmod p^2$ genügt.

Beweis:

$\Rightarrow$: Sei $p|F_n$, also $2^{2^n} \equiv -1 \bmod p$, d.h. die Ordnung von $(2 \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})^*$ ist 2^{n+1} (vgl. Beweis zu Lemma 2.2.1), daher

$$2^{n+1} \mid p - 1 \ .$$

Daraus folgt: $(2^{2^{n+1}} - 1) \mid (2^{p-1} - 1)$, denn allgemein gilt:

$$2^{a\cdot b} - 1 = (2^a - 1)(1 + 2^a + \ldots + 2^{a(b-1)}) \ .$$

Sei nun $p^2|F_n$, d.h. $2^{2^n} \equiv -1 \bmod p^2$.
Daraus folgt: $2^{2^{n+1}} \equiv 1 \bmod p^2$, also

$$p^2 \mid (2^{2^{n+1}} - 1) \quad \text{und damit} \quad p^2 \mid (2^{p-1} - 1) \; .$$

$\Leftarrow$: Um diese Richtung des Satzes zu beweisen, benutze ich das folgende

Lemma 2.5.3
Sei p prim.
Falls $p|(2^m - 1), m \geq 1$ und $p^2 \mid (2^{p-1} - 1)$, dann gilt:

$$p^2 \mid (2^m - 1) \; .$$

Beweis des Lemmas:
Ist r die Ordnung von ($2 \bmod p$), so folgt $r|(p-1), r|m$.
Dann $p - 1 = r \cdot k \quad (*) \quad$ und $\quad 2^r = 1 + c \cdot p$ mit $k,\; c \geq 1$. Damit ist $2^{p-1} = (1 + c \cdot p)^k \equiv 1 + k \cdot c \cdot p \bmod p^2$, d.h. $p^2 \mid (2^{p-1} - 1 - k \cdot c \cdot p)$. Da nach Voraussetzung $p^2|(2^{p-1} - 1)$ und $p \nmid k$ wegen $(*)$, so muß gelten: $p|c$.
Sei nun $m = r \cdot h$ mit $h \geq 1$.
Dann

$$2^m = (1 + c \cdot p)^h \equiv 1 + h \cdot c \cdot p \equiv 1 \bmod p^2 \; .$$

$\square$

Der eigentliche Beweis: Sei

$$p|F_n, \text{ d.h. } p \mid (2^{2^n} + 1) \; .$$

Dann $p \nmid (2^{2^n} - 1)$, d.h. $2^{2^n} \not\equiv 1 \bmod p \quad (**)$, da $p \neq 2$. Aus $p|F_n$ bzw. $2^{2^n} \equiv -1 \bmod p$ folgt auch

$$2^{2^{n+1}} \equiv 1 \bmod p, \qquad \text{also} \qquad p \mid (2^{2^{n+1}} - 1) \; .$$

Da nun nach Voraussetzung gilt: $p^2 \mid (2^{p-1} - 1)$, so folgt nach dem obigen Lemma:

$$p^2 \mid (2^{2^{n+1}} - 1), \qquad \text{d.h.} \qquad 2^{2^{n+1}} \equiv 1 \bmod p^2 \; ,$$

also damit

$$p^2 \mid (2^{2^n} + 1) \qquad \text{bzw.} \qquad 2^{2^n} \equiv -1 \bmod p^2,$$

denn $2^{2^n} \not\equiv 1 \bmod p^2$ wegen $(**)$ $((\mathbb{Z}/p^2\mathbb{Z})^*$ ist zyklisch, hat also nur eine Untergruppe der Ordnung 2).

q.e.d.

Bemerkung:
Man kennt bis heute keinen einzigen Faktor der Fermat-Zahlen, der der

Wieferich-Kongruenz genügt, d.h. man kennt kein Quadrat, welches ein Teiler einer Fermat-Zahl ist.

1093 und 3511 sind die *einzigen* Primzahlen $< 4 \cdot 10^{12}$, die der Wieferich-Kongruenz genügen, also auch die kleinsten, entdeckt 1913 von *Meissner* bzw. 1922 von *Beeger* (vgl. Ribenboim [19] S. 23, Crandall et al. [40]). □

Eine Vorgehensweise, um zu entscheiden, ob die vorliegenden Faktoren der Fermat-Zahlen F_n Primzahlpotenzen sind oder nicht, die auf *Lenstra et al* (vgl. [49]) zurückgeht, ist die folgende:

Nach dem kleinen Fermatschen Satz gilt $a^N \equiv a \bmod N$ für jede Zahl a und jede Primzahl N bzw. N ist zusammengesetzt, falls ein a existiert mit

$$a^N \not\equiv a \bmod N \ .$$

Falls N eine Primzahlpotenz ist, d.h.

$$N = p^k, \quad k > 1 \ ,$$

dann gilt $a^p \equiv a \bmod p$ für alle a und daher auch $a^N = a^{p^k} \equiv a \bmod p$, damit:

$$p|(a^N - a), \qquad \text{also auch} \qquad p|ggT(a^N - a, N) \ .$$

Also: Hat man ein a gefunden mit $(a^N - a \bmod N) \neq 0$, so wird dann $d := ggT(a^N - a \bmod N, N)$ ausgerechnet.

Falls $d = 1$ ist, so läßt sich folgern, daß N keine Primzahlpotenz ist.
Ist $d \neq 1$, dann ist das ein nichttrivialer Faktor von N, was gewöhnlich viel wichtiger ist als die Information, ob N Primzahlpotenz ist oder nicht.

Nun kann man den im vorherigen Abschnitt 2.4 skizzierten Primzahltest von *Suyama* geringfügig so abändern, daß auch zusätzlich die Primzahlpotenz-Struktur der untersuchenden Faktoren der Fermat-Zahlen ausgeschlossen werden kann.

Sei G ein Faktor von F_n, d.h. $F_n = f \cdot G$, dessen Charakter unbekannt ist. Gesucht ist ein a mit $(a^G - a \bmod G) \neq 0$.

Nach *Suyama* gilt ja:
Falls $R^2 \not\equiv 3^{f-1} \bmod G$, so ist G zusammengesetzt, wobei $R = 3^{\frac{F_n - 1}{2}} \bmod F_n$ ist.

Man wählt also $a = 3^f$.

Dann ist

$$\begin{aligned} ggT((3^f)^G - 3^f, g) &= ggT(3 \cdot R^2 - 3^f, G) \\ &= ggT(R^2 - 3^{f-1}, G). \end{aligned}$$

Der Primzahltest von *Suyama* heißt nun:

Auszurechnen ist:

$$d := ggT(R^2 - 3^{f-1}, G) \ .$$

Falls $d = 1$ ist, dann ist G weder prim noch ist G eine Primzahlpotenz.
Auf diese Weise haben *Crandall et al* (vgl. [40]) gezeigt, daß die Faktoren G_{19} und G_{21} von

$$\begin{aligned} F_{19} &= 4561072932012444929229 8 \cdot G_{19} \\ F_{21} &= 4485296422913 \cdot G_{21} \end{aligned}$$

weder prim noch Primzahlpotenzen sind.

3 Einige Faktorisierungsideen

3.1 Einführung

Eine ganze Zahl $N > 1$ ist entweder eine zusammengesetzte Zahl, die als Produkt zweier ganzer Zahlen größer als 1 geschrieben werden kann, oder sie ist eine Primzahl. Zwei fundamentale Probleme in der elementaren Zahlentheorie sind gerade:

1) Von einer gegebenen Zahl $N > 1$ zu entscheiden, ob sie prim oder zusammengesetzt ist und

2) Falls N zusammengesetzt ist, dann $a, b > 1$ zu finden, so daß $N = a \cdot b$.

In den letzten Jahrzehnten sind zu den Problemen der Primzahlerkennung und der Faktorzerlegung große Fortschritte erzielt worden, die durch das Aufkommen leistungsstarker Computer ermöglicht wurden.

Eine erfolgreiche Faktorisierung löst natürlich das Problem der Primzahlerkennung, d.h. jede Faktorisierungsmethode ist auch ein "Nicht-Primzahltest".

Will man nur herausfinden, ob eine gegebene, "große" Zahl prim oder nicht ist, empfiehlt es sich, einen Primzahltest zu benutzen, der sich nicht auf die Faktorisierung dieser Zahl verläßt, da die bekannten Faktorisierungsmethoden "sehr viel langsamer" als die bekannten Primzahltests sind und damit teuerer.

Eine Ausnahme gibt es jedoch, und zwar, falls die Faktoren von der zu untersuchenden Zahl N leicht zu finden sind, z.B. sehr klein sind, kann die Faktorisierung als Nicht-Primzahltest bequem verwendet werden. 76% der ganzen ungeraden Zahlen haben einen Primteiler kleiner als 100 (vgl. Riesel [22]). Man hat also mit der Probedivision durch alle ungeraden Primzahlen < 100 gute Chancen, zu beweisen, daß N zusammengesetzt ist.

Festzuhalten ist aber auf jeden Fall: Wird zu Faktorisierung einer Zahl irgendeine andere Methode verwendet, sollte man sicher sein, daß diese Zahl nicht prim ist.

3.2 Die Fermat'sche Methode

Eine ungerade zusammengesetzte Zahl N besitze eine Faktorzerlegung

$$N = p \cdot q \quad \text{mit} \quad q > p \,.$$

Diese Zahl N kann faktorisiert werden, indem man sie als Differenz von zwei Quadratzahlen schreibt; es gilt nämlich:

$$N = \left(\frac{p+1}{2}\right)^2 - \left(\frac{q-p}{2}\right)^2 = \left(\frac{p+q}{2} + \frac{q-p}{2}\right)\left(\frac{p+q}{2} - \frac{q-p}{2}\right) = q \cdot p\,.$$

Die Suche nach Quadratzahlen, deren Differenz gleich N ist, ist die Faktorisierungsidee von *Fermat*.

Bei diesem Verfahren startet man mit der kleinsten ganzen Zahl $x_0 \geq \sqrt{N}$, bildet die Differenz $z_0 = x_0^2 - N$ und prüft anschließend, ob z_0 eine Quadratzahl y_0^2 ist.

Wenn das der Fall ist, dann:
Aus $x_0^2 - N = y_0^2$ folgt $N = x_0^2 - y_0^2 = (x_0 - y_0)(x_0 + y_0)$, und damit erhält man eine Faktorzerlegung von N.
Andernfalls bildet man für das nächste $x_1 = x_0 + 1$ die Differenz

$$x_1^2 - N = (x_0+1)^2 - N = x_0^2 + 2x_0 + 1 - N = z_0 + 2x_0 + 1$$

und prüft ob $z_1 = z_0 + 2x_0 + 1$ eine Quadratzahl y_1^2 ist. Und so verfährt man weiter, bis man die Faktorzerlegung von N gefunden hat oder bis eine vorgegebene Maximalanzahl der Schritte erreicht ist.

Die Anzahl der nötigen Schritte, um die Faktorzerlegung von N zu finden, läßt sich abschätzen:
Der Anfangswert von x ist $\approx \sqrt{N}$, und bei $x = \frac{p+q}{2}$ ist die Faktorzerlegung von N gefunden. Da $q = \frac{N}{p}$, so ist die Anzahl der nötigen Schritte:

$$\approx \frac{1}{2}(p + \frac{N}{p}) - \sqrt{N} \quad = \quad \frac{(\sqrt{N} - p)^2}{2p}\,. \tag{1}$$

Wenn also p und q annähernd gleich groß sind, d.h. beide "in der Nähe" von $\sqrt{N}$ liegen, dann ist aus (1) ersichtlich, daß die Anzahl der nötigen Schritte, um N zu faktorisieren, relativ klein ist, da der Faktor p in diesem Fall dicht unter $\sqrt{N}$ liegt.
Sei nun $p \approx k \cdot \sqrt{N}, 0 < k < 1$.
Dann folgt aus (1):

$$\frac{(\sqrt{N} - k\sqrt{N})^2}{2 \cdot k\sqrt{N}} = \frac{(\sqrt{N}(1-k))^2}{2k\sqrt{N}} \quad = \quad \frac{(1-k)^2}{2k} \cdot \sqrt{N} \tag{2}$$

Beispiel:
Für $k = 0,001$ ist $\frac{(1-k)^2}{2k} \approx 499$, d.h. nur wenn beide Faktoren nahe bei $\sqrt{N}$ sind, hat die Fermat-Methode einen praktischen Nutzen. □

Bemerkung:
Aus $N = p \cdot q, q > p$ und $p \approx k \cdot \sqrt{N}, 0 < k < 1$ erhält man

$$\begin{aligned} q - p &= \frac{N}{p} - p \approx \frac{N}{k\sqrt{N}} - k\sqrt{N} = \frac{N - k^2 N}{k\sqrt{N}} \\ &= \frac{(1-k^2)N}{k\sqrt{N}} = \frac{(1-k^2)}{k}\sqrt{N} = \alpha \cdot \sqrt{N} \; . \end{aligned}$$

wobei $\alpha := \frac{1-k^2}{k}$ und daraus erhält man

$$k = \frac{\sqrt{4+\alpha^2} - \alpha}{2} \tag{$*$}$$

setzt man $(*)$ in (2) ein, so erhält man nach Zwischenrechnung in Abhängigkeit von α die Anzahl der nötigen Schritte (abgeschätzt), um N zu faktorisieren:

$$\begin{aligned} &\approx \left(\frac{\sqrt{4+\alpha^2}}{2} - 1 \right) \cdot \sqrt{N} = \left(\sqrt{1 + \frac{\alpha^2}{4}} - 1 \right) \cdot \sqrt{N} \\ &\approx \frac{1}{2} \cdot \frac{\alpha^2}{4} \cdot \sqrt{N} \qquad \text{nach } \textit{Taylor}\text{ , wenn } \alpha \text{ klein ist.} \end{aligned}$$

Beispiel:
Zur Faktorisierung einer 50-stelligen Zahl N mit $q - p \approx 0,1\sqrt{N}$ sind $\approx \frac{1}{8} \cdot 10^{-4}\sqrt{N}$ Schritte nötig, d.h. mit $N \leq 10^{50}$ immer noch mindestens 10^{20} Schritte. □

□

Folgendes ist eine *Aribas*-Funktion zur Faktorisierung von N nach dem Fermat-Verfahren mit maximal *anz* Schritten. Dabei ist *Aribas* ein unter MS-DOS lauffähiger *Pascal*-ähnlicher Multipräzisions-Interpreter, der sich auf einer zu Forster [8] beiliegenden Diskette befindet.

Beispiel:
Die Funktion ferm-factorize liefert die Faktorisierung von $10^{22}+1$, nachdem man die trivialen Faktoren 89 und 101 abgespalten hat:

$$N = \frac{10^{22}+1}{89 \cdot 101} = 1112470797641561909 \ .$$

Die nötige Mindestanzahl der Schritte beträgt 1803. Also, mit
ferm-factorize $(N, 1803)$ erhält man:

$$N = 1056689261 \cdot 1052788969.$$

□

Anmerkung zur Aribas-Funktion:
Bei der Feststellung, ob eine Zahl eine Quadratzahl ist, wurde folgende Tatsache benutzt:
Für eine Quadratzahl mod 100 gibt es einen der folgenden 22 möglichen Reste:

$$0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41,$$
$$44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96 \ .$$

Und kürzer können sie geschrieben werden als

$$0, a1, a4, 25, b6, a9,$$

wobei a eine gerade einstellige Ziffer ist und b eine ungerade; dabei ist $a = 0$ zugelassen. □

3.3 Die Kraitchik'sche Methode

1920 führte *Maurice Kraitchik* das Verfahren von *Fermat* weiter aus, und diese Verbesserung ist die Basis vieler moderner Faktorisierungsmethoden. (Diese Idee hat zwar ihre Wurzeln in den Arbeiten von *Seelhoff* aus dem Jahre 1886 (vgl. [63]), aber es war *Kraitchik*, der sie "aus dem Schatten heraus brachte und der neuen Generation in neuem Jahrhundert vorstellte" (vgl. Pomerance [56])).
Anstatt nach Zahlen u und v zu suchen, so daß $u^2 - v^2 = N$, genügt es, u und v so zu wählen, daß $u^2 - v^2$ gleich einem Vielfachen von N ist, daß also

$$(*) \qquad u^2 \equiv v^2 \bmod N \quad \text{gilt} \ .$$

Interessante, d.h. wünschenswerte Lösungen dieser Kongruenz sind solche mit $u \not\equiv \pm\, v \bmod N$, und entsprechend sind die Lösungen $u \equiv \pm\, v \bmod N$

uninteressant. Wenn also eine Lösung u, v der obigen Kongruenz $(*)$ bekannt ist mit $u \not\equiv \pm\, v \bmod N$, so läßt sich daraus eine Zerlegung von N konstruieren, denn aus $(*)$ folgt:

$$(u+v)(u-v) \equiv 0 \bmod N \;.$$

Da vorausgesetzt wurde, daß N keinen der Faktoren teilt, erhält man mit $ggT(u-v, N)$ einen nicht-trivialen Teiler von N.

Was das Verhältnis der wünschenswerten Lösungen, d.h. solchen mit $u \not\equiv \pm\, v \bmod N$ gegenüber der uninteressanten Lösungen angeht, so stelle ich eine heuristische Überlegung auf:

Sei N ungerade mit (mindestens) zwei verschiedenen Primteilern p und q. Dann ist (mindestens) die Hälfte der Lösungen von

$$u^2 \equiv v^2 \bmod N \;,$$

wobei

$$ggT(u \cdot v, N) = 1 \;,$$

von der interessanten Art ist.

Denn: Aus der Kongruenz

$$u^2 \equiv v^2 \bmod N$$

folgt, daß

$$(u+v)(u-v) \equiv 0 \bmod N \;,$$

d.h. N ist ein Teiler von $(u+v)(u-v)$.

Wenn $p \neq q$ und $p|N, q|N$, dann ist die Wahrscheinlichkeit, daß beide $(u-v)$, oder daß beide $(u+v)$ teilen, gleich $\frac{1}{2}$, falls Faktoren $(u-v)\cdot(u+v) = N$ unabhängig und gleichverteilt sind.

Also gilt mit der Wahrscheinlichkeit $\frac{1}{2}$:

$$\begin{array}{lcl} p|(u-v,n) & \text{und} & q \nmid (u-v,N) \quad \text{oder} \\ p \nmid (u-v,N) & \text{und } q|(u-v,N) \;, & \end{array}$$

bzw. mit dieser Wahrscheinlichkeit ist einer von den beiden ein nichttrivialer Teiler von N. □

Sei eine zu faktorisierende Zahl N gegeben.

Nach *Fermat* startet man mit der kleinsten ganzen Zahl $x_0 \geq \sqrt{N}$ und bildet $Q(x) = x^2 - N$ für $x = x_0 + k, k \geq 0$ bis man auf eine Quadratzahl $Q(x) = y^2$ stößt.

Nach *Kraitchik* sucht man nach verschiedenen Zahlen x, so daß das Produkt entsprechender $Q(x)$ eine Quadratzahl ist:

Wenn also

$$Q(x_1) \cdot \ldots \cdot Q(x_k) = v^2$$

und

$$x_1 \cdot \ldots \cdot x_k = u,$$

dann ist

$$u^2 = x_1^2 \cdot \ldots \cdot x_k^2 \equiv (x_1^2 - N) \cdot \ldots \cdot (x_k^2 - N) = Q(x_1) \cdot \ldots \cdot Q(x_k) = v^2 \bmod N\ .$$

Man hat damit eine Lösung zu

$$u^2 \equiv v^2 \bmod N\ .$$

Nun stellt sich das Problem:
Wie kann man aus einer Folge von Zahlen eine Teilmenge $x_1, \ldots, x_k$ finden, so daß das Produkt $Q(x_1) \cdot \ldots \cdot Q(x_k)$ eine Quadratzahl ist?

Falls von den Zahlen $Q(x_1), \ldots, Q(x_k)$ die Primfaktorzerlegung bekannt ist, braucht man nur darauf zu achten, daß im Produkt der Exponent jedes Primfaktors eine gerade Zahl ist. Ich illustriere das am folgenden Beispiel.

Beispiel:
Sei $N = 2461$.
Dann ist $x_0 = 49$ und

$$\begin{aligned}
Q(x_1) &= x_1^2 - N = 50^2 - N = 39 = 3 \cdot 13 \\
Q(x_2) &= x_2^2 - N = 51^2 - N = 140 = 2^2 \cdot 5 \cdot 7 \\
Q(x_3) &= x_3^2 - N = 52^2 - N = 243 = 3^5 \\
Q(x_4) &= x_4^2 - N = 53^2 - N = 348 = 2^2 \cdot 3 \cdot 29 \\
Q(x_5) &= x_5^2 - N = 54^2 - N = 455 = 5 \cdot 7 \cdot 13\ .
\end{aligned}$$

Also:

$$Q(x_1) \cdot Q(x_2) \cdot Q(x_3) \cdot Q(x_5) = (2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13)^2 =: v^2$$

und

$$\begin{aligned}
u &:= 50 \cdot 51 \cdot 52 \cdot 54 \equiv 1351 \bmod 2461 \\
v &= 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \equiv 2421 \bmod 2461\ .
\end{aligned}$$

Da $1351 \not\equiv \pm\ 2421 \bmod 2461$, so hat man mit

$$ggT(2421 - 1351, 2461) = 107$$

einen Teiler von 2461.
Es ist $2461 = 107 \cdot 23$. □

3.4 Die Legendre'sche Methode

Ähnlich wie *Kraitchik* ging auch *Adrien Marie Legendre* (1752 bis 1833) vor ihm von einer Reihe von Kongruenzen $u_i^2 \equiv q_i \bmod N$ aus, um N zu faktorisieren.

Hierbei ist wichtig, wie wir bei *Kraitchik* gesehen haben, genügend leicht zu faktorisierende quadratische Reste $q_i \bmod N$ zur Verfügung zu haben. *Legendre* hatte die Idee, dafür die Kettenbruchentwicklung von $\sqrt{N}$ zu benutzen, denn bei der Kettenbruchentwicklung von $\sqrt{N}$ werden viele quadratische Reste mod N erzeugt.

Ist $\frac{A_i}{B_i}$ der i-te Näherungsbruch der Kettenbruchentwicklung von $\sqrt{N}$, dann ist

$$(-1)^i Q_i = A_{i-1}^2 - B_{i-1}^2 N$$

und damit ist

$$A_{i-1}^2 \equiv (-1)^i Q_i \bmod N$$

d.h. $(-1)^i Q_i$ ist ein quadratischer Rest mod N. (Vgl. hierzu Abschnitt. 4.2, bzw. Satz 4.2.9 .)

Nachdem ausreichend viele quadratische Reste gefunden sind, wird ein Sieb konstruiert, in welchem jeder quadratische Rest über die Hälfte der Primzahlen als mögliche Primteiler von N "vernichtet". Das wird begründet einerseits:

Aus

$$x^2 \equiv a \bmod N$$

folgt

$$x^2 \equiv a \bmod p$$

für jeden Primteiler p von N und andererseits aus dem

Lemma 3.4.1

Modulo einer ungeraden Primzahl p gibt es $\frac{1}{2}(p-1)$ quadratische Reste und ebensoviele quadratische Nichtreste.

Beweis:

Für eine ungerade Primzahl p ist die multiplikative Gruppe $\mathbb{F}_p^*$ des Körpers $\mathbb{F}_p$ mit p Elementen zyklisch von der Ordnung $p-1$. Der Kern des Homomorphismus $\mathbb{F}_p^* \to \mathbb{F}_p^*, x \mapsto x^2$ hat die Ordnung 2.

Das Bild $(\mathbb{F}_p^*)^2$ dieses Homomorphismus hat daher die Ordnung $\frac{(p-1)}{2}$.

Also gibt es in $\mathbb{F}_p^*$ genauso viel Quadrate wie Nichtquadrate:

$$\mathbb{F}_p^* : (\mathbb{F}_p^*)^2 = 2 \;.$$

q.e.d.

Ich illustriere diese Methode am folgenden Beispiel (vgl. Riesel [22], S. 153 f.):

Beispiel:
Sei $N = 12007001$.
Aus der Kettenbruchentwicklung von $\sqrt{N}$ wurden Q_i und A_{i-1} berechnet und für ausgewählte i hat man nun:

$i = 28$: $6764708^2 \equiv 2048 = 2^{11} \bmod N$, daraus folgt:
$a = 2$ ist auch quadratischer Rest mod N.

$i = 6$: $2228067^2 \equiv 40 = 2^3 \cdot 5 \bmod N$, daraus folgt:
$a = 5$ ist quadratischer Rest mod N.

$i = 3$: $31186^2 \equiv -488 = -97 \cdot 5 \bmod N$, daraus folgt:
$a = -97$ ist quadratischer Rest mod N.

$i = 27$: $11477856^2 \equiv -155 = -31 \cdot 5 \bmod N$, daraus folgt:
$a = -31$ ist quadratischer Rest mod N.

$i = 10$: $668093^2 \equiv 1475 = 5^2 \cdot 59 \bmod N$, daraus folgt:
$a = 59$ ist quadratischer Rest mod N.

$i = 45$: $7504807^2 \equiv -1525 = -61 \cdot 5^2 \bmod N$, daraus folgt:
$a = -61$ ist quadratischer Rest mod N.

Da auch gilt:
$$10957^2 \equiv -14161 = -7^2 \cdot 17^2 \bmod N ,$$
so folgt:
$$a = -1 \quad \text{ist quadratischer Rest mod } N ,$$
damit sind also auch $a = 61, 31, 97$ quadratische Reste mod N.
Also: Die folgenden ausgewählten Zahlen sind quadratische Reste mod N:
$$a = -1, 2, 5, 31, 59, 61 \text{ und } 97 .$$
Nun gilt nach den "Ergänzungssätzen" 2.2.3:
Da -1 und 2 quadratische Reste mod N sind, können einerseits nur Primzahlen p der Form $p = 4k + 1$ Teiler von N sein und andererseits nur Primzahlen p einer der beiden Formen $p = 8k \pm 1$.
Damit haben die Primteiler p von N die Form
$$p = 8k + 1 . \qquad (*)$$
Nach dem quadratischen Reziprozitätsgesetz (Satz 2.2.4) bzw. den "Ergänzungssätzen" 2.2.3 gilt:
$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \cdot (-1)^{\frac{p-1}{2}} \text{ und } (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{falls} \quad p \equiv 1 \bmod 4 \\ -1, & \text{falls} \quad p \equiv 3 \bmod 4 , \end{cases}$$

und man hat:

$$\left(\frac{p}{5}\right) = \begin{cases} (\frac{1}{5}) = 1, & \text{falls} \quad p \equiv 1 \bmod 5 \\ (\frac{2}{5}) = -1, & \text{falls} \quad p \equiv 2 \bmod 5 \\ (\frac{3}{5}) = -1, & \text{falls} \quad p \equiv 3 \bmod 5 \\ (\frac{4}{5}) = (-1)\cdot(-1) = 1, & \text{falls} \quad p \equiv -1 \bmod 5\ . \end{cases}$$

Damit: Falls 5 quadratischer Rest mod N ist, dann können nur diejenigen Primzahlen p Teiler von N sein, die eine der vier Formen $p = 20k \pm 1, \pm 9$ haben.

Also haben unter Berücksichtigung von $(*)$ Primteiler p von N die Form

$$p = 40k + 1 \qquad \text{oder} \qquad p = 40k + 9\ .$$

Um nicht in dieser Weise fortzufahren, berechne ich stattdessen für $a = 31, 59, 61$ und 97 das Legendre-Symbol $(\frac{a}{p})$, wobei $p < 3465 = [\sqrt{N}]$ und $p = 40k + 1$ oder $p = 40k + 9$.

Falls also für ein solches p und ein solches a gilt: $(\frac{a}{p}) = -1$, d.h. a quadratischer Nichtrest mod p, wird p als möglicher Primteiler von N eliminiert.

Nun läßt sich relativ leicht ausrechnen, daß es folgende Primzahlen $p < 3465$ der Form $p = 40k + 1$ oder $p = 40k + 9$ mit $(\frac{31}{9}) = +1$ gibt:

$$\begin{aligned} p \;\; = \;\; & 41, 281, 521, 769, 1249, 1289, 1321, 1361, 1409, 1489, 1601, 1609, 1721, \\ & 2081, 2281, 2521, 2609, 2729, 3001, 3089, 3169, 3209, 3449\ . \end{aligned}$$

Unter diesen Primzahlen ist $(\frac{59}{p}) = +1$ für:

$$p = 41, 281, 529, 1361, 1609, 2081, 2729, 3001, 3089 \text{ und } 3449\ .$$

Unter diesen nun ist $(\frac{61}{p}) = +1$ für:

$$p = 41, 1361, 2729, 3001 \text{ und } 3089\ .$$

Von den obigen fünf Primzahlen ist $(\frac{97}{p}) = +1$ nur für 1361 und 3001.

Durch Probedivision kann man nun feststellen, daß $1361 \nmid N$, aber $3001 \mid N$.
In der Tat: $12007001 = 3001 \cdot 4001$. □

4 Faktorisierung mit Kettenbrüchen

4.1 Einführung

Die Kettenbruchmethode, die hier skizziert werden soll, wurde zuerst von *D.H. Lehmer* und *R.E. Powers* 1931 vorgestellt.

Die Inspiration hierzu geht aber schon einerseits auf die Faktorisierungsmethode von *Legendre* zurück, woher die Idee stammt, viele quadratische Reste modulo N aus der Kettenbruchentwicklung von $\sqrt{N}$ zu erzeugen; andererseits geht die Idee, vorhandene Reste zu kombinieren, um neue Reste (in diesem Fall: Quadrate) zu erzeugen, auf die Faktorisierungsmethode von *Kraitchik* zurück.

In gegenwärtige Standardform gebracht, d.h. systematisch die Potentiale dieser Ideen erforscht und auf einem Computer implementiert, wurde die Kettenbruchmethode von *M. Morrison* und *J. Brillhart*. Sie haben mit dieser Methode erfolgreich die Fermatsche Zahl $F_7 = 2^{128} + 1$ am 13. September 1970 faktorisiert. Die Beschreibung der Methode und Ergebnisse der Faktorisierung haben *Morrison* und *Brillhart* 1975 in einem ausführlichen Bericht veröffentlicht (vgl. [52]).

Während der 70er Jahre war die Kettenbruchmethode die "Hauptmethode" zur Faktorisierung großer Zahlen; sie war das schnellste Mittel zur Faktorisierung großer Zahlen mit großen Primfaktoren. Auch heute noch wird die Kettenbruchmethode für Faktorisierungszwecke verwendet.

Bevor ich zu der Beschreibung des Faktorisierungsalgorithmus von *Morrison* & *Brillhart* komme, ist es erforderlich eine kurze Einführung in die allgemeine Theorie der Kettenbrüche zu machen. Dabei stütze ich mich im wesentlichen auf Forster [8].

4.2 Kettenbrüche

Die hier betrachteten Kettenbrüche sind Ausdrücke der Form

$$\mathrm{cfrac}\,(a_0, a_1, \ldots, a_{n-1}, a_n) \quad = \quad a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots\, a_{n-1} + \cfrac{1}{a_n}}}}$$

d.h. mit induktiver Beschreibung:

$$\begin{aligned}
\text{cfrac}\,(a_0) &= a_0 \\
\text{cfrac}\,(a_0, a_1) &= a_0 + \frac{1}{a_1} \\
&\vdots \\
\text{cfrac}\,(a_0, \ldots, a_n) &= a_0 + \frac{1}{\text{cfrac}\,(a_1, \ldots, a_n)} = \text{cfrac}\,(a_0,\ \text{cfrac}\,(a_1, \ldots, a_n))\,.
\end{aligned}$$

Man hat dann die allgemeine Schachtelungsformel

$$\text{cfrac}\,(a_0, \ldots, a_n) = \text{cfrac}\,(a_0, \ldots, a_k,\ \text{cfrac}\,(a_{k+1}, \ldots, a_n))\,.$$

Natürlich ist ein Kettenbruch nur definiert, wenn die auftretenden Nenner nicht Null sind.

Kettenbrüche treten auf, wenn man die reellen Zahlen x wie folgt approximiert:

$$\alpha_0 = x, \quad a_0 = [\alpha_0]$$

($[\alpha_0]$ bedeutet Gauß-Klammer, d.h. die größte ganze Zahl $\leq \alpha_0$.)

$$\begin{aligned}
&\text{Falls} \quad \alpha_0 \notin \mathbb{Z}: \quad x = a_0 + \frac{1}{\alpha_1} \ \text{ mit } \ \alpha_1 > 1 \qquad \text{also} \\
&\qquad\qquad\qquad\quad x = \text{cfrac}\,(a_0, \alpha_1). \\
&\text{Falls} \quad \alpha_1 \notin \mathbb{Z}: \quad a_1 = [\alpha_1] \geq 1, \alpha_1 = a_1 + \frac{1}{\alpha_2} \ \text{ mit } \ \alpha_2 > 1 \qquad \text{also} \\
&\qquad\qquad\qquad\quad x = \text{cfrac}\,(a_0, a_1, \alpha_2).
\end{aligned}$$

Auf diese Weise erhält man ganze Zahlen $a_0, a_1, \ldots$ (mit $a_i \geq 1$ für $i \geq 1$) und reelle Zahlen $\alpha_1, \alpha_2, \ldots$ (mit $\alpha_1 > 1$ für $i \geq 1$), so daß stets

$$x = \text{cfrac}\,(a_0, a_1, \ldots, a_n, \alpha_{n+1})\,.$$

Das Verfahren bricht ab mit dem ersten Index r, für den $\alpha_r \in \mathbb{Z}$:
Dann hat man $a_r = \alpha_r$ und also

$$x = \text{cfrac}\,(a_0, \ldots, a_r)\,.$$

Wenn aber $\alpha_r \notin \mathbb{Z}$, so fährt man fort:

$$a_r = [\alpha_r], \alpha_r = a_r + \frac{1}{\alpha_{r+1}}$$

und erhält

$$x = \text{cfrac}\,(a_0, \ldots, a_r, \alpha_{r+1})\,.$$

Beispiele:

1.
$$\frac{54}{19} = 2 + \frac{16}{19} = 2 + \frac{1}{1 + \frac{3}{16}} = 2 + \frac{1}{1 + \frac{1}{5+\frac{1}{3}}} = \text{ cfrac } (2, 1, 5, 3).$$

2. Um die Kettenbruchentwicklung von $\sqrt{2}$ zu ermitteln, kann man ausgehen von
$$(\sqrt{2} - 1)(\sqrt{2} + 1) = 1, \quad \text{also } \sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}} \ .$$
Damit ergibt sich:
$$\begin{aligned} \sqrt{2} &= 1 + \frac{1}{1+\sqrt{2}} = \text{ cfrac } (1, 1 + \sqrt{2}) \\ &= 1 + \cfrac{1}{2 + \cfrac{1}{1+\sqrt{2}}} = \text{ cfrac } (1, 2, 1 + \sqrt{2}) \\ &= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1+\sqrt{2}}}} = \text{ cfrac } (1, 2, 2, 1 + \sqrt{2}) \ , \end{aligned}$$
und induktiv fortfahrend erhält man die periodische Entwicklung:
$$\sqrt{2} = \text{ cfrac } (1, 2, 2, 2, \dots) \ .$$

□

Satz 4.2.1 *:*
Die Kettenbruchentwicklung von $x \in \mathbb{R}$ bricht genau dann ab, wenn x eine rationale Zahl ist.

Beweis:

$\Rightarrow$: Hat man $x = \text{cfrac } (a_0, \dots, a_n)$ mit ganzen Zahlen a_i, so ist x offenbar eine rationale Zahl.

$\Leftarrow$: Sei x rational, d.h. $x = \frac{u_0}{u_1}$ mit teilerfremden ganzen Zahlen u_0, u_1 und $u_1 > 0$.
Der euklidische Algorithmus liefert dann:
$$\begin{aligned} u_0 &= a_0 u_1 + u_2 && (0 < u_2 < u_1) \\ u_1 &= a_1 u_2 + u_3 && (0 < u_3 < u_2) \\ &\vdots \\ u_{n-1} &= a_{n-1} u_n + u_{n+1} && (0 < u_{n+1} < u_n) \\ u_n &= a_n \cdot u_{n+1} \end{aligned}$$

Dabei gilt $a_k = \left[\frac{u_k}{u_{k+1}}\right]$, also mit $x_k = \frac{u_k}{u_{k+1}}$:

$$x_k = a_k + \frac{u_{k+2}}{u_{k+1}} = a_k + \frac{1}{x_{k+1}} \; .$$

Das heißt:

$$x = x_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{x_2}} = \ldots = \text{ cfrac } (a_0, \ldots, a_n),$$

wegen $\quad x_n = \frac{u_n}{u_{n+1}} = a_n.$

q.e.d.

Jede *irrationale reelle Zahl* x hat also eine *unendliche Kettenbruchentwicklung*

$$x = \text{ cfrac } (a_0, a_1, \ldots, a_n, \ldots) \; .$$

Dabei gilt nach Konstruktion:

$$a_i \in \mathbb{Z} \qquad \text{und} \qquad a_i \geq 1 \quad \text{für} \quad i \geq 1,$$

und es gibt *Restzahlen* $\alpha_i > 1$ mit

$$x = \text{ cfrac } (a_0, \ldots, a_n, \alpha_{n+1}),$$

wobei dann $\alpha_{n+1} = \text{cfrac } (a_{n+1}, a_{n+2}, \ldots)$.

Die rationale Zahl

$$\frac{u_n}{v_n} = \text{ cfrac } (a_0, \ldots, a_n)$$

heißt *n-ter Näherungsbruch* zu x.

Bemerkung:

Wegen $a + 1 = a + \frac{1}{1}$ ist die Kettenbruchentwicklung einer Bruchzahl nicht eindeutig, wenn man als letzte Zahl 1 zuläßt:

$$\begin{aligned} \text{cfrac } (a_0, a_1, \ldots, a_{n-1} + 1) &= \text{cfrac } (a_0, a_1, \ldots, a_{n-1}, 1) \quad \text{und} \\ \text{cfrac } (a_0, a_1, \ldots, a_{n-1}, a_n) &= \text{cfrac } (a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1) \end{aligned}$$

falls $a_n > 1$, denn $a_n = a_n - 1 + \frac{1}{1}$.

Um Eindeutigkeit zu erreichen, schließt man in der Regel 1 als letzte Zahl in einem Kettenbruch aus. □

Das folgende Lemma zeigt, daß die Einführung der zweidimensionalen Vektor-Matrixschreibweise überaus nützlich für die Theorie der Kettenbrüche ist.

Lemma 4.2.2

Sei $x = \text{cfrac}\,(a_0, a_1, \ldots, a_n, \frac{\alpha}{\beta})$ mit $a_i, \alpha, \beta \in \mathbb{R}, \beta > 0$.
Dann gilt $x = \frac{u}{v}$, wobei

$$\binom{u}{v} := A_0 \cdot \ldots \cdot A_n \binom{\alpha}{\beta} \quad \text{und} \quad A_k := \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Beweis:

Per Induktion nach $n \geq 0$. Induktionsanfang $n = 0$:

$$\begin{aligned} x = \text{ cfrac}\,(a_0, \frac{\alpha}{\beta}) &= a_0 + \frac{1}{\frac{\alpha}{\beta}} = a_0 + \frac{\beta}{\alpha} = \frac{a_0\alpha + \beta}{\alpha} \\ &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \binom{\alpha}{\beta} = A_0 \binom{\alpha}{\beta}. \end{aligned}$$

Induktionsschritt: Nach Induktionsvoraussetzung gilt:

$$x' := \text{ cfrac}\,(a_1, \ldots, a_n, \frac{\alpha}{\beta}) = \frac{u'}{v'}$$

mit $\binom{u'}{v'} = A_1 \cdot \ldots \cdot A_n \binom{\alpha}{\beta}$.
Daraus folgt

$$x = \text{ cfrac}\,(a_0, \frac{u'}{v'}) = a_0 + \frac{1}{\frac{u'}{v'}} = \frac{a_0 u' + v'}{u'} = \frac{u}{v}$$

mit

$$\binom{u}{v} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \binom{u'}{v'} = A_0 \cdot A_1 \cdot \ldots \cdot A_n \binom{\alpha}{\beta}.$$

q.e.d.

Das Lemma dient uns dazu, die gekürzte Darstellung von Näherungsbrüchen zu ermitteln:

Satz 4.2.3

Seien $a_0, a_1, \ldots, a_n, \ldots$ ganze Zahlen mit $a_i \geq 1$ für $i \geq 1$.
Setzt man für $n \geq 0$:

$$\frac{u_n}{v_n} = \text{ cfrac}\,(a_0, \ldots, a_n) \quad \text{mit} \quad v_n > 0$$

und teilerfremden u_n, v_n, so gilt für $n > 0$:

$$\begin{bmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{bmatrix} = A_0 \cdot A_1 \cdot \ldots \cdot A_n, \quad \text{wobei} \quad A_k = \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix}.$$

Insbesondere folgt wegen $\det A_k = -1$:

$$u_n v_{n-1} - u_{n-1} v_n = (-1)^{n+1}, \qquad (4.2.3i)$$

und wegen

$$\begin{bmatrix} u_{n+1} & u_n \\ v_{n+1} & v_n \end{bmatrix} = A_0 \cdot \ldots \cdot A_n \cdot A_{n+1} = \begin{bmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{bmatrix} \begin{bmatrix} a_{n+1} & 1 \\ 1 & 0 \end{bmatrix}$$

hat man die folgenden *Rekursionsformeln* für Zähler und Nenner:

$$\begin{aligned} u_{n+1} &= a_{n+1} u_n + u_{n-1} \\ v_{n+1} &= a_{n+1} v_n + v_{n-1} \,. \end{aligned} \qquad (4.2.3.ii)$$

□

Beweis des Satzes:
Mit $\hat{u}_0 = a_0$ und $\hat{v}_0 = 1$ bildet man:

$$\begin{bmatrix} \hat{u}_n \\ \hat{v}_n \end{bmatrix} = A_0 \cdot \ldots \cdot A_{n-1} \begin{bmatrix} a_n \\ 1 \end{bmatrix} \,.$$

Nach dem Lemma 4.2.2 gilt:

$$\text{cfrac}\,(a_0, \ldots, a_n) = \frac{\hat{u}_n}{\hat{v}_n} \,.$$

und man verifiziert sofort, daß $\hat{v}_n > 0$.
Wegen

$$\begin{bmatrix} a_{n-1} \\ 1 \end{bmatrix} = A_{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

hat man auch

$$\begin{bmatrix} \hat{u}_{n-1} \\ \hat{v}_{n-1} \end{bmatrix} = A_0 \cdot \ldots \cdot A_{n-2} \begin{bmatrix} a_{n-1} \\ 1 \end{bmatrix} = A_0 \cdot \ldots \cdot A_{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \,,$$

so daß insgesamt gilt:

$$\begin{bmatrix} \hat{u}_n & \hat{u}_{n-1} \\ \hat{v}_n & \hat{v}_{n-1} \end{bmatrix} = A_0 \cdot \ldots \cdot A_{n-1} \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix} = A_0 \cdot \ldots \cdot A_{n-1} \cdot A_n \,.$$

Mit $\det A_k = -1$ folgt auch

$$\hat{u}_n \hat{v}_{n-1} - \hat{u}_{n-1} \hat{v}_n = (-1)^{n+1} \,.$$

daher sind $\hat{u}_n$ und $\hat{v}_n$ teilerfremd, und es ergibt sich:

$$u_n = \hat{u}_n, \; v_n = \hat{v}_n \,.$$

q.e.d.

Mein Ziel ist es, Genaueres über die Kettenbruchentwicklung einer irrationalen reellen Zahl x zu erfahren. Deshalb zuerst der folgende

Satz 4.2.4
Sei $x \in \mathbb{R} - \mathbb{Q}$.
Mit dem n-ten Näherungsbruch $\frac{u_n}{v_n} = \text{cfrac}\,(a_0, \ldots, a_n)$ und der $(n+1)$-ten Restzahl α_{n+1} gilt:

$$x = \frac{u_n \alpha_{n+1} + u_{n-1}}{v_n \alpha_{n+1} + v_{n-1}}$$

und

$$x - \frac{u_n}{v_n} = \frac{(-1)^n}{v_n(v_n \alpha_{n+1} + v_{n-1})} \; .$$

Beweis:
Aus $x = \text{cfrac}\,(a_0, \ldots, a_n, \alpha_{n+1})$
folgt mit Lemma 4.2.2., daß $x = \frac{u}{v}$, wobei

$$\begin{pmatrix} u \\ v \end{pmatrix} = A_0 \cdot \ldots \cdot A_n \begin{pmatrix} \alpha_{n+1} \\ 1 \end{pmatrix}, A_k = \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \; .$$

Und da zusätzlich nach Satz 4.2.3

$$A_0 \cdot \ldots \cdot A_n = \begin{pmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{pmatrix}$$

gilt, ist damit die erste Formel des Satzes bewiesen.
Damit erhält man dann

$$\begin{aligned} x - \frac{u_n}{v_n} = \frac{u_n \alpha_{n+1} + u_{n-1}}{v_n \alpha_{n+1} + v_{n-1}} - \frac{u_n}{v_n} &= \frac{v_n u_{n-1} - u_n v_{n-1}}{v_n(v_n \alpha_{n+1} + v_{n-1})} \\ &= \frac{(-1)^n}{v_n(v_n \alpha_{n+1} + v_{n-1})} \end{aligned}$$

nach der Folgerung (4.2.3 *i*).

q.e.d.

Nach Konstruktion gilt:

$$a_{k+1} = [\alpha_{k+1}] \quad \text{und} \quad \alpha_{k+1} > a_{k+1}, \quad \text{da } x \in \mathbb{R} - \mathbb{Q} \; .$$

Also gilt nun:

$$\frac{1}{v_n(v_n \alpha_{n+1} + v_{n-1})} < \frac{1}{v_n(v_n a_{n+1} + v_{n-1})} \overset{(*)}{=} \frac{1}{v_n v_{n+1}}$$

($(*)$: folgt aus den Rekursionsformeln 4.2.3. *ii.*)
Es folgt daher

$$x - \frac{u_n}{v_n} = \frac{(-1)^n \cdot \epsilon}{v_n \cdot v_{n+1}} \quad \text{mit} \quad 0 < \epsilon < 1, \epsilon \in \mathbb{R} \; .$$

Für $x \in \mathbb{R} - \mathbb{Q}$ gilt also

$$x = \lim_{n \to \infty} \frac{u_n}{v_n} \quad \text{bzw.}$$
$$\left| x - \frac{u_n}{v_n} \right| \quad < \quad \frac{1}{v_n \cdot v_{n+1}} \quad < \quad \frac{1}{v_n^2} \, .$$

Und es gilt auch

$$\left| x - \frac{u_n}{v_n} \right| \quad < \quad \frac{1}{a_{n+1} \cdot v_n^2} \, ,$$

denn nach den Rekursionsformeln gilt

$$v_{n+1} = a_{n+1} \cdot v_n + v_{n-1} > a_{n+1} \cdot v_n, \quad \text{da} \quad v_i > 0 \quad \text{für alle} \quad i \, .$$

Ein n-ter Näherungsbruch $\frac{u_n}{v_n}$ zu x ist also eine gute Approximation, falls a_{n+1} relativ groß ist.

Beispiel:

(Vgl. auch Loxton [16], S. 88.)

Ich betrachte die Kettenbruchentwicklung von π:

$$\pi = \text{ cfrac } (3, 7, 15, 1, 292, 1, \ldots).$$

Es gilt dann:

$$\text{cfrac } (3,7) = \frac{22}{7} \quad , \quad \text{cfrac } (3,7,15,1) = \frac{355}{113} \quad \text{und}$$
$$\left| \pi - \frac{22}{7} \right| < \frac{1}{15 \cdot 7^2} \quad , \quad \left| \pi - \frac{355}{113} \right| < \frac{1}{292 \cdot 113^2} \, .$$

$\frac{355}{113}$ ist also eine gute Approximation für π. □

Periodische Kettenbrüche

Definition 4.2.5

Ein unendlicher Kettenbruch cfrac $(a_0, a_1, \ldots, a_n, \ldots)$ heißt *periodisch*, wenn die Folge der Elemente $a_0, a_1, \ldots$ periodisch ist. Es gibt dann eine *Vorperiode*: $a_0, \ldots, a_{n_0 - 1}$ und eine *Periode*: $a_{n_0}, \ldots, a_{n_0+k-1}$, d.h. es existieren ein kleinstes $k > 0$ und ein $n \geq 0$ so, daß $a_{n+k} = a_n$ für alle $n \geq n_0$ gilt.

k heißt *Periodenlänge*. Dafür schreibt man:

$$\text{cfrac } (a_0, a_1, \ldots, a_{n_0-1}, \, \overline{a_{n_0}, \ldots, a_{n_0+k-1}}) \, .$$

Für $n_0 = 0$ heißt der Kettenbruch *rein periodisch*.

Notiz:
Sei $x \in \mathbb{R} - \mathbb{Q}$ durch einen periodischen Kettenbruch dargestellt.
Dann gilt für die Restzahlen

$$\alpha_{n_0} = \alpha_{n_0+k}$$

wegen $\alpha_{n_0} = \text{cfrac}\,(a_{n_0}, a_{n_0+1}, \ldots) = \text{cfrac}\,(a_{n_0+k}, a_{n_0+1+k}, \ldots) = \alpha_{n_0+k}$.
Umgekehrt ist die Kettenbruchentwicklung von x periodisch, wenn für ein gewisses n_0 gilt:

$$\alpha_{n_0} = \alpha_{n_0+k} \quad (k \geq 1) .$$

Denn: Es gilt dann

$$a_{n_0} + \frac{1}{\alpha_{n_0+1}} = a_{n_0+k} + \frac{1}{\alpha_{n_0+k+1}}$$

und so ist (wegen $\alpha_{n_0+\nu} = \alpha_{n_0+k+\nu}, \nu = 0, 1, 2, \ldots$)

$$a_{n_0} = a_{n_0+k} \quad \text{bzw.} \quad a_n = a_{n+k} \quad \text{für} \quad n \geq n_0 .$$

□

Ich komme nun zu der Frage, welche reellen bzw. irrationalen Zahlen eine periodische Kettenbruchentwicklung besitzen. Vollständige Auskunft gibt der folgende Satz, der auf *Euler* und *Lagrange* zurückgeht:

Satz 4.2.6
Die Kettenbruchentwicklung einer irrationalen Zahl x ist genau dann periodisch, wenn x eine quadratische Irrationalzahl ist, wenn also x nicht rational und Lösung einer Gleichung $y^2 + c_1 y + c_2 = 0$ mit $c_1, c_2 \in \mathbb{Q}$ ist.

Ich werde nur eine Richtung des Beweises zeigen, in welcher man für den nächsten Abschnitt wichtige Erkenntnisse gewinnt.

Beweis:

$\Leftarrow$: Sei x eine quadratische Irrationalzahl, also $x = \frac{a+\sqrt{b}}{c}$ mit $a, b, c \in \mathbb{Z}$, wobei $c \neq 0, b > 0$ und b keine Quadratzahl ist. Falls noch nicht $c|(b - a^2)$ gilt, kann man erweitern:

$$x = \frac{ac \pm \sqrt{bc^2}}{c^2} = \frac{P_0 + \sqrt{d}}{Q_0} \quad \text{mit} \quad P_0, d, Q_0 \in \mathbb{Z} ,$$

$Q_0 \neq 0, d > 0, d$ keine Quadratzahl und $Q_0|(d - P_0^2)$.

Für $k \geq 0$ werden die Reste α_k in $x = \operatorname{cfrac}(a_0, \ldots, a_{k-1}, \alpha_k)$ induktiv in der Form $\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$ mit ganzen Zahlen P_k und $Q_k \neq 0$, so daß $Q_k | d - P_k^2$ gilt, konstruiert, beginnend mit

$$\alpha_0 = x = \frac{P_0 + \sqrt{d}}{Q_0} .$$

Hat man α_k schon erhalten, so setzt man

$$P_{k+1} = a_k Q_k - P_k$$

und rechnet:

$$d - P_{k+1}^2 = d - a_k^2 Q_k^2 + 2a_k Q_k P_k - P_k^2 = d - P_k^2 + Q_k(2a_k P_k - a_k^2 Q_k) .$$

Daher kann man setzen

$$Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$$

und hat $Q_k \cdot Q_{k+1} = d - P_{k+1}^2$, also $Q_{k+1} \neq 0$, da d keine Quadratzahl ist. Für α_{k+1} ergibt sich nun

$$\begin{aligned} \alpha_{k+1} &= \frac{P_{k+1} + \sqrt{d}}{Q_{k+1}} = \frac{Q_k(P_{k+1} + \sqrt{d})}{d - P_{k+1}^2} = \frac{Q_k}{\sqrt{d} - P_{k+1}} \\ &= \frac{Q_k}{\sqrt{d} - a_k Q_k + P_k} = \frac{1}{\alpha_k - a_k} \qquad \text{d.h} \\ \alpha_k &= a_k + \frac{1}{\alpha_{k+1}} , \end{aligned}$$

so daß in der Tat gilt:

$$x = \operatorname{cfrac}(a_0, \ldots, a_k, \alpha_{k+1}) .$$

Es bleibt noch zu zeigen, daß diese Kettenbruchentwicklung periodisch ist. Dafür wird nachgewiesen, daß die P_k und Q_k beschränkt sind.
Also: Für

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$$

sei

$$\overline{\alpha_n} = \frac{P_k - \sqrt{d}}{Q_k}$$

die konjugierte Zahl.
Sind $\frac{u_k}{v_k}$ die Näherungsbrüche der Kettenbruchentwicklung von x, so gilt nach Satz 4.2.4:

$$\begin{aligned} x &= \frac{u_k \alpha_{k+1} + u_{k-1}}{v_k \alpha_{k+1} + v_{k-1}} \qquad \text{und damit} \\ \bar{x} &= \frac{u_k \overline{\alpha_{k+1}} + u_{k-1}}{v_k \overline{\alpha_{k+1}} + v_{k-1}} . \end{aligned}$$

Da
$$\begin{pmatrix} u_k & u_{k-1} \\ v_k & v_{k-1} \end{pmatrix}^{-1} = (-1)^{k+1} \begin{pmatrix} v_{k-1} & -u_{k-1} \\ -v_k & u_k \end{pmatrix} ,$$
so folgt
$$\overline{\alpha_{k+1}} = \frac{v_{k-1}\bar{x} - u_{k-1}}{-v_k\bar{x} + u_k} = -\frac{v_{k-1}}{v_k} \cdot \left(\frac{\bar{x} - \frac{u_{k-1}}{v_{k-1}}}{\bar{x} - \frac{u_k}{v_k}} \right) .$$
Für $k \to \infty$ konvergiert die Klammer in der oberen Zeile gegen $1 = \frac{\bar{x}-x}{\bar{x}-x}$.
Für $k \geq k_0$ ist also $\overline{\alpha_k} < 0$.
Nach Konstruktion hat man $\alpha_k > 1$, also:
$$0 < \alpha_k - \overline{\alpha_k} = \frac{2\sqrt{d}}{Q_k} \quad \text{für } k \geq k_0 ,$$
insbesondere $Q_k > 0$ für $k \geq k_0$.
Weiterhin folgt mit $Q_k \cdot Q_{k-1} = d - P_k^2$ für $k > k_0$:
$$\begin{aligned} P_k^2 &= d - Q_k \cdot Q_{k-1} < d && \text{und da} \\ 1 < \alpha_k &= \frac{P_k + \sqrt{d}}{Q_k} \quad \text{für} \quad k > 0, \end{aligned}$$
folgt also
$$Q_k < P_k + \sqrt{d} < 2\sqrt{d} .$$
Daher gibt es nur endlich viele Möglichkeiten für α_k, es muß also Indizes $k_2 > k_1$ geben mit $\alpha_{k_2} = \alpha_{k_1}$.
Daraus folgt die Periodizität des Kettenbruchs von x.

q.e.d.

Anmerkungen:

1. Kettenbruchentwicklung ist hier mit ganzzahliger Arithmetik wegen der Rekursion für die P_k und Q_k.
2. Wegen $0 < Q_k < 2\sqrt{d}$ und $0 < P_k < \sqrt{d}$ können also Q_k und P_k nur endlich viele Werte annehmen und daher ist die Perioden länge hier abschätzbar $< 2\sqrt{d} \cdot \sqrt{d} = 2d$ (vgl. die Bemerkung auf Seite 52f). □

Um die Kettenbruchentwicklung von $\sqrt{N}$ für eine positive ganze Zahl N, die kein Quadrat ist, angeben zu können, brauche ich noch den folgenden, hier nicht zu beweisenden

Satz 4.2.7

Die Kettenbruchentwicklung einer quadratischen Irrationalzahl x ist rein periodisch genau dann, wenn $x > 1$ und $-1 < \bar{x} < 0$, wobei für

$$\begin{aligned} x &= \text{cfrac}\,(\overline{a_0, a_1, \ldots, a_{n-1}, a_n}) \\ -\frac{1}{\bar{x}} &= \text{cfrac}\,(\overline{a_n, a_{n-1}, \ldots, a_1, a_0}) \end{aligned}$$

ist. □

Nach diesen Vorbereitungen kann man nun zeigen, daß die Kettenbruchentwicklung von Quadratwurzeln eine sehr spezielle Form hat:

Satz 4.2.8

Ist $N > 1$ eine natürliche Zahl, die kein Quadrat ist, dann ist

$$\sqrt{N} = \text{cfrac}\,(\omega, \overline{a_1, \ldots, a_{n-1}, 2\omega})\ ,$$

wobei $\omega = [\sqrt{N}]$ und $a_{n-i} = a_i$ für $i = 1, \ldots, n-1$.
Umgekehrt stellt jeder derart symmetrische Kettenbruch eine Quadratwurzel dar.

Beweis:

$\Rightarrow$: Sei so eine Zahl $N > 1$ gegeben, sei $\omega = [\sqrt{N}]$ und $x = \omega + \sqrt{N}$

Dann ist nach Satz 4.2.7 die Kettenbruchentwicklung von x rein periodisch, da

$$x > 1 \quad \text{und} \quad -1 < \bar{x} < 0, \quad \text{denn} \quad \bar{x} = \omega - \sqrt{N}\ .$$

Also:

$$\begin{aligned} x &= \omega + \sqrt{N} = \text{cfrac}\,(\overline{2\omega, a_1, \ldots, a_{n-1}}) \quad \text{mit} \\ a_0 &= [x] = 2\omega \quad \text{und} \quad x = 2\omega + \frac{1}{\alpha_1} \end{aligned}$$

und damit

$$\sqrt{N} = x - \omega = \text{cfrac}\,(\omega, \overline{a_1, \ldots, a_{n-1} 2\omega})$$

denn

$$x - \omega = \omega + \frac{1}{\alpha_1}\ .$$

Es ist noch die Symmetrie $a_{n-i} = a_i$ zu beweisen:
Da

$$\begin{aligned} x &= \text{cfrac}\,(\overline{2\omega, a_1, \ldots, a_{n-1}}), \qquad \text{so ist} \\ \frac{1}{x - 2\omega} &= \text{cfrac}\,(\overline{a_1, \ldots, a_{n-1}, 2\omega})\ . \end{aligned}$$

Nach Satz 4.2.7 ist dann

$$\begin{aligned} \text{cfrac}\,(\overline{2\omega, a_{n-1}, \ldots, a_1}) &= \frac{-1}{(\frac{1}{x-2\omega})} = -(\bar{x} - 2\omega) \\ = 2\omega - \bar{x} = 2\omega - (\omega - \sqrt{N}) &= \omega + \sqrt{N} = x = \text{cfrac}\,(\overline{2\omega, a_1, \ldots, a_{n-1}})\,. \end{aligned}$$

Wegen der Eindeutigkeit der Kettenbruchentwicklung ist die Behauptung bewiesen.

$\Leftarrow$: Nach der nicht bewiesenen Richtung von Satz 4.2.6 ist x eine quadratische Irrationalzahl der Gestalt

$$x = u + v\sqrt{d} \quad \text{mit} \quad u, v \in \mathbb{Q}\,.$$

Ist nun $x = \text{cfrac}\,(\omega, \overline{a_1, \ldots, a_{n-1}, 2\omega})$,
dann ist

$$\frac{1}{x-\omega} = \text{cfrac}\,(\overline{a_1, \ldots, a_{n-1}, 2\omega})$$

und nach Satz 2.4.7:

$$-\frac{1}{(\frac{1}{x-\omega})} = \omega - \bar{x} = \text{cfrac}\,(\overline{2\omega, a_{n-1}, \ldots, a_1})\,,$$

also

$$-\bar{x} = \text{cfrac}\,(\omega, \overline{a_{n-1}, \ldots, a_1, 2\omega}) = \text{cfrac}\,(\omega, \overline{a_1, \ldots, a_{n-1}, 2\omega})$$

wegen der vorausgesetzten Symmetrie.
Also gilt:

$$\begin{aligned} x = -\bar{x}, &\quad \text{d.h.} \quad u + v\sqrt{d} = -u + v\sqrt{d} \qquad \text{und damit} \\ u = 0 &\quad \text{bzw.} \quad x = v\sqrt{d} = \sqrt{v^2 d}\,. \end{aligned}$$

q.e.d.

Bemerkung:
Für eine positive ganze Zahl N ist die Kettenbruchentwicklung von $\sqrt{N}$ der Form:

$$\sqrt{N} = \text{cfrac}\,(a_0, \overline{a_1, \ldots, a_\ell}),$$

wobei

$$a_0 = [\sqrt{N}] \text{ und } a_\ell = 2a_0\,.$$

Ein interessantes Problem ist die Periodenlänge ℓ, "gut" abzuschätzen.
T. Vijayaraghavan (vgl. Ayoub et al [29]) hat gezeigt, daß für die Periodenlänge ℓ gilt:

$$\ell = O(\sqrt{N}\log N)$$

für alle $N > 0$, und:

$$\ell > N^{\frac{1}{2}-\delta}$$

für unendlich viele $N > 0$, wobei $\delta > 0$ willkürlich klein.

In [67] zeigten *R.G. Stanton, C. Sudler, Jr.* und *H.C. Williams*, daß für alle quadratfreie $N > 7$ gilt:

$$\ell < 0,72\sqrt{N}\log N\ .$$

1931 wurde von *S. Chowla* und *S.S. Pillai* (in [38]) gezeigt, daß unter gewissen Bedingungen

$$\ell = O(\sqrt{N}\log\log N)$$

gilt; und es existieren positive Konstanten C_1 und C_2 so, daß gilt:

$$C_1\sqrt{N} < \ell < C_2\sqrt{N}$$

für unendlich viele $N > 0$.

Weiterhin zeigten sie, daß "im Durchschnitt" die Periodenlänge ℓ der Ordnung $\sqrt{N}$ ist. (Vgl. hierzu die Beispiele im Anhang.) □

Die Kettenbruchmethode baut auf dem folgenden Satz auf:

Satz 4.2.9

Für $\sqrt{N}$ = cfrac $(a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0})$ sei $\frac{A_k}{B_k}$ der k-te Näherungsbruch (A_k, B_k teilerfremd und $B_k > 0$) und $\alpha_{k+1} = \frac{P_{k+1}+\sqrt{N}}{Q_{k+1}}$ die $(k+1)$-te Restzahl.

Dann gilt:

$$A_k^2 - NB_k^2 = (-1)^{k+1}Q_{k+1}\ .$$

Beweis:

Wegen Satz 4.2.4 gilt

$$\sqrt{N} = \frac{A_k\alpha_{k+1} + A_{k-1}}{B_k\alpha_{k+1} + B_{k-1}} = \frac{A_kP_{k+1} + A_k\sqrt{N} + A_{k-1}Q_{k+1}}{B_kP_{k+1} + B_k\sqrt{N} + B_{k-1}Q_{k+1}}$$

bzw.

$$B_kN + \sqrt{N}(B_kP_{k+1} + B_{k-1}Q_{k+1}) = (A_kP_{k+1} + A_{k-1}Q_{k+1}) + A_k\sqrt{N}\ .$$

In Matrizen-Schreibweise ist das

$$\begin{pmatrix} B_kN \\ A_k \end{pmatrix} = \begin{pmatrix} A_k & A_{k-1} \\ B_k & B_{k-1} \end{pmatrix} \begin{pmatrix} P_{k+1} \\ Q_{k+1} \end{pmatrix}.$$

Da

$$\begin{pmatrix} A_k & A_{k-1} \\ B_k & B_{k-1} \end{pmatrix}^{-1} = (-1)^{k+1} \begin{pmatrix} B_{k-1} & -A_{k-1} \\ -B_k & A_k \end{pmatrix},$$

so ist also

$$(-1)^{k+1}\begin{pmatrix} B_{k-1} & -A_{k-1} \\ -B_k & A_k \end{pmatrix} \begin{pmatrix} B_k N \\ A_k \end{pmatrix} = \begin{pmatrix} P_{k+1} \\ Q_{k+1} \end{pmatrix},$$

d.h. man erhält die Behauptung in der zweiten Komponente.

q.e.d.

4.3 Faktorisierungsalgorithmus von Morrison & Brillhart

Die Methode wird in drei Schritten erklärt:

Schritt 1:

Sei $N > 1$ eine ungerade zusammengesetzte Zahl, die kein Quadrat ist.

Für $\sqrt{N}$ oder $\sqrt{\mu N}$, wobei $1 \leq \mu < N$ eine ganze Zahl ist (die Rolle dieses Multiplikators μ wird später erklärt), wird die Kettenbruchentwicklung berechnet:

$$\sqrt{\mu N} = \text{ cfrac } (a_0, a_1, \ldots, a_k, \alpha_{k+1})$$

bis zu einem gewisen $k = k_0 - 1$, wobei

$$\alpha_{k+1} = \frac{\sqrt{\mu N} + P_{k+1}}{Q_{k+1}}$$

die $(k+1)$-te Restzahl ist.

Nach Satz 4.2.9 gilt für jedes $k, 0 \leq k \leq k_0 - 1$:

$$A_k^2 - \mu N B_k^2 = (-1)^{k+1} Q_{k+1} ,$$

wobei $\frac{A_k}{B_k}$ der k-te Näherungsbruch ist.

Daraus folgt gleich:

$$A_k^2 \equiv (-1)^{k+1} Q_{k+1} \bmod N .$$

Zu beachten ist:

Auch wenn man die Kettenbruchentwicklung von $\sqrt{\mu N}$ statt $\sqrt{N}$ berechnet, es wird immer modulo N reduziert.

Ein Zahlenpaar $(A_{k-1} \bmod N, Q_k)$ für $1 \leq k \leq k_0$ in der obigen Kongruenz wird von *Morrison* und *Brillhart* ein "$A - Q$-Paar" genannt.

Zur Berechnung der Kettenbruchentwicklung von $\sqrt{\mu N}$ werden die im Beweis des Satzes 4.2.6 abgeleiteten Formeln verwendet, und zwar:

Mit $a_0 := [\sqrt{\mu N}]$ ist hier

$$\alpha_0 = \sqrt{\mu N} = \frac{0 + \sqrt{\mu N}}{1}, \quad \text{also} \quad P_0 = 0, Q_0 = 1$$

$$\alpha_0 = a_0 + \frac{1}{\alpha_1}, \quad \text{d.h.} \quad \alpha_1 = \frac{1}{\sqrt{\mu N} - a_0} = \frac{a_0 + \sqrt{\mu N}}{\mu N - a_0^2}$$
$$\text{also} \quad P_1 = a_0, Q_1 = \mu N - a_0^2$$

und die Teilbarkeitsbedingung ist trivialerweise erfüllt.

Mit $\alpha_k = \frac{\sqrt{\mu N}+P_k}{Q_k}$ gilt

$$a_k := [\alpha_k] = \left[\frac{a_0 + P_k}{Q_k}\right] \quad \text{für} \quad k \geq 1 \, ,$$

und man hat die Rekursionsformeln:

$$\begin{aligned} P_{k+1} &= a_k Q_k - P_k \\ Q_{k+1} &= Q_{k-1} + a_k(P_k - P_{k+1}) \, . \end{aligned}$$

Für die Berechnung von $A_k \bmod N$ schließlich hat man nach Folgerung aus dem Satz 4.2.3 die Rekursionsformel:

$$A_k \equiv a_k A_{k-1} + A_{k-2} \bmod N \quad \text{mit} \quad A_{-2} = 0 \quad \text{und} \quad A_{-1} = 1 \, .$$

Die Nenner der Näherungsbrüche müssen also nicht berechnet werden.
Mit der Berechnung zur Kettenbruchentwicklung von $\sqrt{\mu N}$ hört man spätestens dann auf, wenn das Ende der Periode erreicht ist, d.h. sobald ein Koeffizient mit $a_k = 2a_0$ auftaucht. (Wie wir unter "Bemerkung" auf Seite 52 schon gesehen haben, ist die Periodenlänge der Kettenbruchentwicklung von $\sqrt{\mu N}$ für die meisten Zahlen N approximativ $\sqrt{\mu N}$.)

Beispiel 4.3.1
Sei $N = 5332777$ und $\mu = 1$. Dann:

k	P_k	Q_k	a_k	A_{k-1} mod N	Q_k faktorisiert
0	0	1	2309	1	/
1	2309	1296	3	2309	$2^4 \cdot 3^4$
2	1579	2191	1	6928	$7 \cdot 313$
3	612	2263	1	9237	$31 \cdot 73$
4	1651	1152	3	16165	$2^7 \cdot 3^2$
5	1805	1801	2	57732	1801
6	1797	1168	3	131629	$2^4 \cdot 73$
7	1707	2071	1	452619	$19 \cdot 109$
8	364	2511	1	584248	$3^4 \cdot 31$
9	2147	288	15	1036867	$2^5 \cdot 3^2$
10	2173	2121	2	138922	$3 \cdot 7 \cdot 101$
11	2069	496	8	1314711	$2^4 \cdot 31$
12	1899	3481	1	5323833	59^2
13	1582	813	4	1305767	$3 \cdot 271$
$\vdots$					

□

Bemerkung:
Wie wir bereits wissen, ist die Kettenbruchentwicklung von $\sqrt{N}$ immer periodisch. Nun in den Fällen, wo die Periode von $\sqrt{N}$ zu kurz ist und nicht genügend quadratische Reste mod N produziert werden und damit die Methode nicht zum Erfolg führen kann, ist es notwendig einen Multiplikator $\mu > 1$ einzuführen und stattdessen die Kettenbruchentwicklung von $\sqrt{\mu N}$ zu berechnen, wie das der Fall ist bei den Fermat-Zahlen F_n.

Die Kettenbruchentwicklung von F_n hat nämlich die Periodenlänge 1.

Um das zu sehen, sei $a = 2^{2^{n-1}}$ bzw. dann $F_n = a^2 + 1$.

Dann gilt:

$$\sqrt{F_n} = \sqrt{a^2+1} = \text{ cfrac } (a, \overline{2a})\,.$$

Denn:

$$\begin{aligned}\sqrt{a^2+1} - a &= \frac{1}{\dfrac{1}{\sqrt{a^2+1}-a}} = \frac{1}{\dfrac{\sqrt{a^2+1}+a}{(\sqrt{a^2+1}-a)(\sqrt{a^2+1}+a)}}\\ = \frac{a^2+1-a^2}{\sqrt{a^2+1}+a} &= \frac{1}{\sqrt{a^2+1}+a} = \frac{1}{2a+(\sqrt{a^2+1}-a)}\,.\end{aligned}$$

(Vgl. hierzu auch die Beispiele im Anhang Teil B.) □

Schritt 2:

Grob skizziert würde dieser Schritt so lauten:
Man suche in der in Schritt 1 erzeugten Menge der $A-Q$-Paare nach gewissen "zulässigen" Untermengen, welche die Eigenschaft haben, daß das

Produkt $\prod_i (-1)^i Q_i$ ihrer Q_i eine Quadratzahl ist. Falls keine solche Untermenge existiert, kehrt man zum Schritt 1 zurück und entwickelt den Kettenbruch von $\sqrt{\mu N}$ weiter.
Um diesen Schritt präziser zu beschreiben, wird zuerst folgendes definiert:
Die Kettenbruchentwicklung

$$\sqrt{\mu N} = \text{ cfrac } (a_0, \ldots, a_{k_0-1}, a_{k_0})$$

liefert Kongruenzen

$$A_{k-1}^2 \equiv (-1)^k Q_k \bmod N \quad \text{für} \quad k = 1, \ldots, k_0 \; .$$

Ein Zahlenpaar $(A_{k-1} \bmod N, Q_k)$ aus der obigen Kongruenz wurde ein $A-Q$-Paar genannt. Nun heißt eine Menge S *zulässig*, wenn $S \subset$ Menge der $A-Q$-Paare und $\prod_{i \in J} (-1)^i Q_i$ ist eine Quadratzahl mit $J \subset \{1, \ldots, k_0\}$ und $(A_{i-1} \bmod N, Q_i) \in S$ für jedes $i \in J$.

Die Bestimmung und Suche nach den zulässigen Mengen in diesem Schritt erfordert, daß in der Menge der $A-Q$-Paare die Q_k vollständig faktorisiert sind. Deshalb wird etwas zur Faktorisierung dieser Q_k gesagt bevor eine systematische Strategie zum Finden der zulässigen Mengen beschrieben wird, denn nicht alle in Schritt 1 erzeugten Q_k werden vollständig faktorisiert, da diese Methode schneller arbeitet, wenn nur besonders einfach zu faktorisierende Q_k berücksichtigt werden, d.h. solche Q_k, die nur Primfaktoren unterhalb einer gewissen Schranke enthalten.

A. Zur Faktorisierung der $\mathbf{Q_k}$

Die Faktorisierung von Q_k ist sehr zeitraubend; für die meisten der zu faktorisierenden Zahlen erfordert sie mehr als 90% der Gesamtlaufzeit.

Anstatt alle in Schritt 1 erzeugten Q_k vollständig zu faktorisieren, werden die Q_k mit großen Primfaktoren, d.h. oberhalb einer vorgegebenen Schranke, ignoriert, weil dadurch die Laufzeit wesentlich verkürzt wird. Der Nutzen jedes einzelnen Q_k stützt sich darauf, ob man eine diesen Index k enthaltende zulässige Menge finden kann; aber ein großer Primteiler p eines Q_k hat wenig Chancen, mit einer geraden Potenz zu erscheinen bzw. eine gerade Potenz zu erhalten. Es ist unwahrscheinlich, daß die Kettenbruchentwicklung mindestens zwei verschiedene Q_k, die jeweils dieses p als Primteiler haben, in angemessener Zeit findet.

Morrison und *Brillhart* gehen bei der Faktorisierung von Q_k wie folgt vor: Wie mehrfach erwähnt, werden nur solche Q_k faktorisiert, deren Primfaktoren unterhalb einer gewissen Schranke B liegen. Für die möglichen ungeraden Primteiler p von Q_k gibt es eine Einschränkung von großer praktischer Bedeutung:

Satz 4.3.2

Sei die Kettenbruchentwicklung von $\sqrt{\mu N}$ gegeben und sei p ein ungerader Primteiler von $Q_k, k \geq 1$. Dann ist das Legendre-Symbol
$(\frac{\mu N}{p})$ gleich 0 oder 1.

Beweis:
Nach Satz 4.2.9 gilt:

$$A_{k-1}^2 - \mu N B_{k-1}^2 = (-1)^k Q_k \ .$$

Sei nun p ein ungerader Primteiler von Q_k. Dann folgt:

$$A_{k-1}^2 \equiv \mu N B_{k-1}^2 \bmod p \ .$$

Da $ggT(A_{k-1}, B_{k-1}) = 1$, kann p nicht B_{k-1} teilen.
Also:

$$\left(\frac{A_{k-1}}{B_{k-1}}\right)^2 \equiv \mu N \bmod p$$

und damit ist μN quadratischer Rest mod p.
Falls nun $p|\mu N$, so ist das Legendre-Symbol $(\frac{\mu N}{p}) = 0$, andernfalls $(\frac{\mu N}{p}) = 1$.
q.e.d.

Bemerkung:
Im Fall $(\frac{\mu N}{p}) = 0$ gibt es eigentlich nur die Möglichkeit, daß $p|\mu$, da man von der Annahme: $p \nmid N$ ausgeht, denn andernfalls hat man schon einen Teiler von N, was ja das Ziel der ganzen Methode ist. □

Nun wird aus der Zahl $p_0 = -1$, der Primzahl $p_1 = 2$ sowie allen ungeraden Primzahlen $p_2, \ldots, p_{r-1}$ bis zu der vorgegebenen Schranke B, für die $(\frac{\mu N}{p})$ gleich 0 oder 1, eine sog. *Faktorbasis* gebildet. (Die Zahl $p_0 = -1$ wird in der Faktorbasis mit eingeschlossen, um zu vermeiden, daß negative Quadrate entstehen, da die einzelnen Q_k auch negativ sein können.)

Die große praktische Bedeutung des obigen Satzes liegt also darin, daß die Dichte der Primzahlen in der Faktorbasis durch die Einschränkung sehr viel kleiner ist als die Dichte aller Primzahlen.

Mit der Faktorbasis kann man nun genauer sagen:
Nur solche Q_k aus einem $A-Q$-Paar werden berücksichtigt, die sich durch die Zahlen $p_0, p_1, \ldots, p_{r-1}$ der Faktorbasis faktorisieren lassen. Für solche Q_k erhält man die Darstellung:

$$A_{k-1}^2 \equiv (-1)^k Q_k = \prod_{0 \leq i < r} p^{\nu_{k_i}} \ .$$

Bemerkung:

Die späteren Versionen dieser Faktorisierungsmethode enthalten eine die Gesamtlaufzeit verkürzende Verfeinerung der Faktorbasis, und zwar baut sie auf der Tatsache auf, daß die Faktorisierung eines Q_k im wesentlichen vollständig ist, nachdem der zweitgrößte Primfaktor dieses Q_k gefunden wurde:

Sei P größter Teiler eines Q_k, der ein Potenzprodukt von Primzahlen in der Faktorbasis ist und p_λ sei die größte in P enthaltende Primzahl.

$\frac{Q_k}{P}$ ist dann Produkt von Primzahlen $> p_\lambda$; gilt daher $\frac{Q_k}{P} < p_\lambda^2$ oder sogar $\frac{Q_k}{P} < p_{r-1}^2$, wobei p_{r-1} die größte Primzahl in der Faktorbasis ist (natürlich kann $p_\lambda = p_{r-1}$ sein), so muß $\frac{Q_k}{P} =: q$ schon eine Primzahl sein.

q ist dann der größte Primteiler von Q_k und p_λ der zweitgrößte.

Da p_{r-1}^2 im allgemeinen "ziemlich groß" ist, wird eine obere Schranke (UB) (engl. upper bound) eingeführt, so daß nun nur solche Q_k berücksichtigt werden, die entweder ganz über der Faktorbasis zerfallen, oder deren Primfaktoren, außer dem größten, in der Faktorbasis liegen, und wobei der größte kleiner ist als UB.

Der Vorteil dieser Abänderung ist der, daß nun eine viel kleinere Faktorbasis verwendet werden kann und somit durch weniger Divisionen die Menge der faktorisierten Q_k erzeugt werden kann.

Bestimmung der optimalen Werte für die Anzahl der Primzahlen in der Faktorbasis (FB) und die obere Schranke (UB) ist hauptsächlich eine Sache der Erfahrung. Welche Werte *Morrison* und *Brillhart* benutzt haben, zeigt die folgende Tabelle:

Anzahl der Dezimalstellen von N	FB	UB
≤ 20	60	3000
21-23	150	10000
24,25	200	14400
26-28	300	22500
29,30	400	29000
31,32	450	36000
33,34	500	36000
35,36	550	36000
37,38	600	44000
39,40	650	53000
41-46	700-1000	63000

□

B. Zur Suche nach zulässigen Mengen

Nun stellt sich die Frage, wie man eine zulässige Menge effizient finden kann oder warum überhaupt sollte so eine Menge existieren?

Die Antwort auf diese Frage gibt uns leicht die Lineare Algebra.
Jede positive ganze Zahl m hat einen zugehörigen Exponentenvektor $\nu(m)$,

der auf der Primfaktorzerlegung von m basiert.
Bezeichne p_j die j-te Primzahl, so ist $m = \prod_j p_j^{\nu_j}$.

Das Produkt durchläuft alle Primzahlen, aber nur endlich viele Exponenten ν_j sind $\neq 0$. Der Exponentenvektor $\nu(m)$ wird dann durch
$\nu(m) := (\nu_1, \nu_2, \ldots)$ definiert.

Ich interessiere mich hier nur für Quadratzahlen und es ist klar, daß eine Zahl m genau dann eine Quadratzahl ist, wenn jede Komponente in $\nu(m)$ gerade ist. Da es also für die Kombination der Q_k zu einer Quadratzahl nur darauf ankommt, ob die zugehörigen Exponenten $(\nu_{k_1}, \nu_{k_2}, \ldots)$ gerade oder ungerade sind, werden diese modulo 2 reduziert.

Also: In diesem Fall wird zuerst für $i = 0, 1, \ldots, r-1$,
$\beta_{k_i} := \nu_{k_i} \bmod 2 \in \mathbb{F}_2$ definiert und anschließend wird der Vektor

$$\vec{\gamma}_k := (\beta_{k_0}, \beta_{k_1}, \ldots, \beta_{k_{r-1}}) \in \mathbb{F}_2^r$$

zusammen mit dem zugehörigen $A-Q$-Paar (d.h. $A_{k-1} \bmod N$ und Q_k) gespeichert.

An dieser Stelle kann nun die Aufgabe dieses Schrittes verdeutlicht werden, da ja auch die Darstellung (aus Teil A.) gilt:

$$A_{k-1}^2 \equiv (-1)^k Q_k = \prod_{0 \leq i \leq r-1} p^{\nu_{k_i}} \ .$$

Die Suche nach einer zulässigen Menge, bzw. nach einer Teilmenge der Q_k, deren Produkt eine Quadratzahl ist, ist mit der Suche nach den zugehörigen Exponentenvektoren, deren Summe gleich dem Nullvektor mod 2 ist, gleichzusetzen.

Da $\mathbb{F}_2^r$ die Dimension r hat, können höchstens r der Vektoren $\vec{\gamma}_k \in \mathbb{F}_2^r$ linear unabhängig sein. Man findet einen Vektor $\vec{\gamma}_k$, der von vorher berechneten Vektoren linear abhängig ist, also spätestens beim $(r+1)$-ten faktorisierten Q_k. Damit existiert dann eine nichttriviale Darstellung der Null, d.h. es gibt Indizes $k_1, \ldots, k_n$ mit

$$\vec{\gamma}_{k_1} + \ldots + \vec{\gamma}_{k_n} = \vec{0} \in \mathbb{F}_2^r \ .$$

Damit ist das Produkt $\prod_{j=1}^n Q_{k_j}$ eine Quadratzahl, und damit ist eine zulässige Menge gefunden worden.

Bemerkung (vgl. Forster [8]):

Die Feststellung der linearen Abhängigkeit dieser Vektoren aus $\mathbb{F}_2^r$, die zusammen mit dem zugehörigen $A-Q$-Paar gespeichert werden müssen, wird mit dem Gauß'schen Eliminationsverfahren durchgeführt.

Seien etwa Vektoren $v_1, v_2, \ldots, v_m \in \mathbb{F}_2^r$ gegeben. Dann wird die $m \times r$-Matrix A mit den Zeilen v_i gebildet, die anschließend mit der Einheitsmatrix

E_m zu einer $m \times (r+m)$-Matrix $M := (A, E_m)$ ergänzt wird. Um nun die Matrix A auf Zeilenstufen-Form zu bringen, werden elementare Zeilenumformungen gleichzeitig auf die beiden Matrizen A und E_m angewendet, und aus M entstehe so die Matrix: $M' = (A', C)$. Da Linksmultiplikation mit $m \times m$-Matrizen Zeilenumformungen bewirkt, so muß die $m \times m$-Matrix C die Umformungsmatrix sein, es gilt also $C \cdot A = A'$. Bezeichnung c_i die i-te Zeile von C und ist die i-te Zeile von A' gleich Null, so gilt also $c_i \cdot A = 0$.

In unserem Fall bedeutet das: Die Summe derjenigen Zeilen von A ist 0, für welche die entsprechenden Komponenten von c_i den Wert 1 haben. □

Ein (unrealistisches) Beispiel zu dem in diesem Schritt beschriebenen Verfahren mit einer kleinen siebenstelligen Zahl wird nach der kurzen Beschreibung des letzten Methodenschrittes präsentiert.

Schritt 3

Mit jeder in Schritt 2 gefundenen zulässigen Menge gilt die Kongruenz:

$$A^2 \equiv \prod_i A_{i-1}^2 \equiv \prod_i (-1)^i Q_i = Q^2 \bmod N \; .$$

wobei $1 \le A < N$.

Zu bestimmen sind dann A und Q in der jeweiligen Kongruenz, damit man schließlich $ggT(A-Q, N)$ bilden kann. Falls $1 < ggT(A-Q, N) < N$ für irgendeine zulässige Menge, dann war die Methode erfolgreich, und dieser ggT ist ein nichttrivialer Teiler von N. Andernfalls geht man zu Schritt 1 zurück.

Beispiel 4.3.3

Hierfür greife ich nochmal das Beispiel 4.3.1 auf, und zwar soll $N = 5332777$ und $\mu = 1$ sein. Die Faktorbasis bestehe aus der Zahl -1 und den Primzahlen $p \le 73$, wobei für das Legendre-Symbol $(\frac{N}{p}) = 1$ gelte. Da zusätzlich im Beispiel 4.3.1 die Q_k für $0 \le k \le 13$ auch faktorisiert wurden, kann die Faktorbasis weiter eingeschränkt werden, und zwar bestehe sie aus den Zahlen

$$-1, 2, 3, 31, 59 \quad \text{und} \quad 73 \; .$$

Dann sind die Ergebnisse der Faktorisierung der Q_k für ausgewählte k in den folgenden Vektorenwerten zu finden:

k	$(-1)^k Q_k$	-1	2	3	31	59	73
1	$-2^4 \cdot 3^4$	1	0	0	0	0	0
3	$-31 \cdot 73$	1	0	0	1	0	1
4	$2^7 \cdot 3^2$	0	1	0	0	0	0
6	$2^4 \cdot 73$	0	0	0	0	0	1
8	$3^4 \cdot 31$	0	0	0	1	0	0

Zwar gibt es mehr Zahlen in der Faktorbasis nämlich 6 als es Zeilenvektoren nämlich 5 gibt, trotzdem besteht zwischen diesen Zeilenvektoren lineare Abhängigkeit, und zwar ist die Summe der

$$1., 2., 4., 5.\ \text{Zeile mod 2 der Nullvektor}\,.$$

Also gilt:

$$A_0^2 \cdot A_2^2 \cdot A_5^2 \cdot A_7^2 \equiv (-Q_1) \cdot (-Q_3) \cdot Q_6 \cdot Q_8 \bmod N$$

d.h.

$$(2309 \cdot 9237 \cdot 131629 \cdot 584248)^2 \equiv (2^4 \cdot 3^4 \cdot 31 \cdot 73)^2 \bmod N$$

bzw.

$$2399929^2 \equiv 2932848^2 \bmod N\,.$$

Da jedoch $ggT(2932848 - 2399929, N) = 1$, ist diese gefundene zulässige Menge nutzlos.
Um weitere zulässige Mengen finden zu können, sind weitere faktorisierte Q_k aus der Kettenbruchentwicklung von $\sqrt{\mu N}$ erforderlich:

k	$(-1)^k Q_k$	-1	2	3	31	59	73
1	$-2^4 \cdot 3^4$	1	0	0	0	0	0
3	$-31 \cdot 73$	1	0	0	1	0	1
4	$2^7 \cdot 3^2$	0	1	0	0	0	0
6	$2^4 \cdot 73$	0	0	0	0	0	1
8	$3^4 \cdot 31$	0	0	0	1	0	0
9	$-2^5 \cdot 3^2$	1	1	0	0	0	0
11	$-2^4 \cdot 31$	1	0	0	1	0	0

Die bestehenden linearen Abhängigkeiten sind hier:

1) Die Summe der 1., 3., 6. Zeile ist der Nullvektor und damit ist eine weitere zulässige Menge gefunden worden. Es gilt:

$$A_0^2 \cdot A_3^2 \cdot A_8^2 \equiv (Q_1) \cdot Q_4 \cdot (-Q_9) \bmod N$$

d.h.

$$(2309 \cdot 16165 \cdot 1036867)^2 \equiv (2^8 \cdot 3^4)^2 \bmod N$$

bzw.

$$5312041^2 \equiv 20736^2 \bmod N\,.$$

Da auch hier $ggT(5312041 - 20736, 5332777) = 1$ gilt, ist man auch mit dieser zulässigen Menge erfolglos.

2) Betrachtet man den 7. Zeilenvektor oben, so stellt man auch dessen lineare Abhängigkeit von den übrigen, und zwar: Die Summe der 1., 5., 7. Zeile ist der Nullvektor.

Es gilt also

$$A_0^2 \cdot A_7^2 \cdot A_{10}^2 \equiv (-Q_1) \cdot Q_8 \cdot (-Q_{11}) \bmod N ,$$

d.h.

$$(2309 \cdot 584248 \cdot 1314711)^2 \equiv (2^4 \cdot 3^4 \cdot 31)^2 \bmod N$$

bzw.

$$5292599^2 \equiv 40178^2 \bmod N .$$

Da auch hier $5292599 \equiv -40178 \bmod 5332777$, denn $5292599+40178 = 5332777$, so ist die Lösung auch uninteressant, bzw. ist

$$ggT(5292599 - 40178, N) = 1 .$$

Da man bis hierhin ohne Erfolg blieb, muß man weiter mit Kettenbruchentwicklung von $\sqrt{\mu N}$ fortfahren. Und als nächstes erhält man ein Quadrat:

k	$(-1)^k Q_k$	-1	2	3	31	59	73
12	59^2	0	0	0	0	0	0

Damit gilt:

$$A_{11}^2 \equiv Q_{12} \bmod N$$

d.h.

$$5323833^2 \equiv 59^2 \bmod N .$$

Nun hat man den Erfolg, denn

$$ggT(5323833 - 59, 5332777) = 3001 \quad \text{und} \quad 3001$$

ist ein Primteiler von N. Also:

$$N = 5332777 = 3001 \cdot 1777 .$$

Anmerkung:
Mit diesem Beispiel habe ich Glück gehabt, denn auf ein Q_k zu stoßen, welches ein Quadrat ist, so daß das Ganze zum Erfolg führt, ist wohl eher eine Ausnahme. Hierzu vergleiche die Beispiele im Anhang, Teil C. □

□

Da in diesem Schritt $ggT(A - Q, N)$ zu berechnen ist, genügt es, anstatt A und Q nur A modulo N und Q modulo N zu kennen. A modulo N wird berechnet, indem man beim Produkt der geeigneten A_i nach jeder

Multiplikation modulo N reduziert.
Bei Q dagegen muß beachtet werden, daß Q^2 nicht modulo N reduziert wird, d.h. ehe die Quadratwurzel nicht gezogen ist, ist die Reduktion modulo N nicht durchführbar. Den Wert Q modulo N kann man natürlich direkt ausrechnen, indem man das Produkt Q^2 bildet, die Quadratwurzel zieht und anschließend das Ergebnis modulo N reduziert. Dieser Weg ist aber unpraktisch, es ist ein zeitraubender Prozeß, da das Produkt Q^2 eine "große" Zahl ist. Im Gegensatz zu direkter Berechnung gibt es einen indirekten Weg, der den Vorteil des Rechnens mit Restklassen ausnützt. Die Idee ist die folgende:

Seien die $Q_{i_1}, \ldots, Q_{i_s}$ aus einer zulässigen Menge gegeben. Das Produkt P dieser Q_i wird zuerst auf $P_1 = Q_{i_1}$ und die Quadratwurzel modulo N wird $\sqrt{R_1} = 1$ "gesetzt".

Als nächstes soll Q_{i_2} zum "Produkt" P_1 multipliziert werden. Falls aber $ggT(P, Q_{i_2}) = X$ ist, wird das "neue" Produkt P_2 anstatt $P_1 \cdot Q_{i_2}$ nun $(\frac{P_1}{X}) \cdot (\frac{Q_{i_2}}{X})$ gleichgesetzt: $P_2 = (\frac{P_1}{X}) \cdot (\frac{Q_{i_2}}{X})$.

Dadurch wird also $P_1 \cdot Q_{i_2}$ reduziert. Den Faktor X multipliziert man zu $\sqrt{R_1}$ und erhält damit die "neue" Quadratwurzel modulo N:

$$\sqrt{R_2} = \sqrt{R_1} \cdot X = X \ .$$

In dieser Weise verfährt man weiter bis zum Produkt P_s und $\sqrt{R_s}$. Falls $P_s = 1$ ist, so ist $\sqrt{R_s}$ die gesuchte Quadratzahl modulo N. Sonst ist P_s eine Quadratzahl (denn das Produkt der Q_i aus einer zulässigen Menge ist eine Quadratzahl und diese Methode ist gerade so angelegt) und dann lautet die gesuchte Quadratwurzel modulo N : $\sqrt{R_s} \cdot \sqrt{P_s}$.
Ich verdeutliche dieses am folgenden

Beispiel 4.3.4

Es soll die Quadratwurzel von $Q_1 \cdot Q_6 \cdot Q_8 \cdot Q_3$ modulo N berechnet werden, wobei die einzelnen Q_i und N aus Beispiel 4.3.3 genommen wurden, d.h. die Quadratwurzel von

$$1296 \cdot 1168 \cdot 2511 \cdot 2263 \bmod 5332777$$

ist auszurechnen. Dann ist: $P_1 = 1296$ und $\sqrt{R_1} = 1$

$$\begin{array}{lll} ggT(1296, 1168) = 16, & P_2 = \frac{1296}{16} \cdot \frac{1168}{16} = 5913, & \sqrt{R_2} = 16 \\ ggT(5913, 2511) = 81, & P_3 = \frac{5913}{81} \cdot \frac{2511}{81} = 2263, & \sqrt{R_3} = 16 \cdot 81 = 1296 \\ ggT(2263, 2263) = 2263, & P_4 = 1, & \sqrt{R_4} = 1296 \cdot 2263 = 2932848. \end{array}$$

Also ist 2932848 die gesuchte Quadratwurzel modulo N, was wir bereits aus Beispiel 4.3.3 kennen. □

4.4 Zum numerischen Ergebnis der Faktorisierung von F_7

1905 haben *Morehead* und *Western* (vgl. [51]) mit dem Satz 2.4.3 von *Pepin* bewiesen, daß die Fermat-Zahl

$$F_7 = 2^{128} + 1 = 340282366920938463463374607431768211457$$

zusammengesetzt ist.

Am 13. September 1970 haben *Morrison* und *Brillhart* diese Zahl in Primfaktoren zerlegt:

$$F_7 = 59649589127497217 \cdot 5704689200685129054721 \ .$$

Als Mutiplikator wurde $\mu = 257$ ausgewählt, wobei man bei der Wahl darauf achtete, daß sowohl die Periode der Kettenbruchentwicklung von $\sqrt{\mu F_7}$ "lang genug" ist als auch kleine Primzahlen in der Faktorbasis zu gewähren. Von den ersten 1330000 der Q_k der Kettenbruchentwicklung von $\sqrt{257 F_7}$ wurden nur 2059 vollständig faktorisiert. Die Kongruenzen der ersten vier zulässigen Mengen blieben erfolglos beim Versuch, F_7 zu faktorisieren. Erst mit Hilfe der Kongruenz

$$\begin{aligned} & 2335036483808358521772321436182279564 76^2 \\ \equiv \ & 2518647814572804129731227193485202122 23^2 \bmod F_7 \end{aligned}$$

wurde F_7 faktorisiert.

Die Faktorisierung von F_7 nahm damals zwar etwa 90 Minuten in Anspruch, aber das Ganze wurde über einen Zeitraum von sieben Wochen ausgeführt. Und heute dagegen kann man z.B. auf einem PC mit schnellem Pentium-Prozessor mit Hilfe von *ARIBAS* das Faktorisierungsergebnis von F_7 schon nach einigen Minuten erhalten (vgl. Forster [8], S. 216).

5 Zusammenstellung von Primfaktoren der Fermat-Zahlen

Die Fermat-Zahlen F_0, F_1, F_2, F_3 und F_4 sind Primzahlen. Die nächsten neunzehn, d.h. F_5 bis einschließlich F_{23} sind keine Primzahlen und von weiteren 116 Fermat'schen Zahlen weiß man auch, daß sie zusammengesetzt sind, d.h. von 135 verschiedenen Fermat-Zahlen weiß man, daß sie zusammengesetzt sind und davon hat man von 132 mindestens einen Primfaktor gefunden.

Nur F_5 bis einschließlich F_{11} sind vollständig faktorisiert, nämlich:

Tabelle 1: *Primfaktoren p der Fermat-Zahlen $F_n, 5 \leq n \leq 11$*

n	p	Entdeckt von
5	$641 \cdot 6700417$	Euler (1732)
6	$274177 \cdot$ 67280421310721	Landry (1880) Landry (1880)
7	$59649589127417217 \cdot$ 5704689200685129054721	Morrison, Brillhart (1970) Morrison, Brillhart (1970)
8	$1238926361552897 \cdot$ p_{62}	Brent, Pollard (1980) Brent, Pollard (1980)
9	$2424833 \cdot$ $p_{49} \cdot p_{99}$	Western (1903) Lenstra et al (1990)
10	$45592577 \cdot$ $6487031809 \cdot$ $p_{40} \cdot p_{252}$	Selfridge (1953) Brillhart (1962) Brent (1995)
11	$319489 \cdot 974849 \cdot$ $167988556341760475137 \cdot$ $3560841906445833920513 \cdot$ p_{564}	Cunningham (1899) Brent (1988) Brent (1988) Brent, Morain (1988)

(p_k bedeutet einen Primfaktor mit k-Stellen)

Lucas benutzte den Satz 2.4.3 von *Pepin* um zu zeigen ,daß F_6 zusammengesetzt ist; und im Alter von 82 Jahren faktorisierte *Landry* diese 20-stellige Zahl, aber seine Methode hat er nicht veröffentlicht.

In [69] gibt *Williams* eine Rekonstruktion der von *Landry* angewendeten Faktorisierungsmethode, die auf den Hinweisen in Briefen und Arbeiten von *Landry* basiert. (Angeblich hat *Clausen*, bekannt als ein wichtiger Astronom, schon 1856 F_6 faktorisiert; dieses wurde aber nie veröffentlicht, vgl. Ribenboim [21], S. 85).

Brent und *Pollard* benutzten eine Version der Pollard'schen Rho-Methode (auch Monte-Carlo-Faktorisierungsmethode genannt), um $F_8 = 2^{256} + 1$ zu faktorisieren (vgl. [33]). Daß der 62-stellige Faktor prim ist, wurde zuerst von *Williams* bewiesen.

1967 bewies *Brillhart*, daß $\frac{F_9}{2424833} =: c_{148}$ eine Zahl mit 148 Dezimalstellen zusammengesetzt ist. Diese Zahl widerstand mehreren Faktorisierungsversuchen mittels Rho-Methode, Pollard'schen $(p \pm 1)$-Methode, Kettenbruchmethode und auch mittels des mehrfach-polynomialen quadratischen Siebes ($MPQS$). Faktorisiert wurde diese Zahl von *Lenstra, Lenstra, Manasse* und *Pollard* (vgl. [49]) mit dem sog. Zahlkörper-Sieb, d.h. mit einer Faktorisierungsmethode, die vom Rechnen in einem algebraischen Zahlkörper, in diesem Fall $Q(\sqrt[5]{2})$ abhängt. Die Rechnungen hierzu wurden auf etwa 700 in aller Welt verstreute "workstations" verteilt, zusätzlich wurde ein Supercomputer eingesetzt. Die gesamte Faktorisierungsarbeit nahm 4 Monate in Anspruch.

F_{10} wurde erst 1995 von *Brent* faktorisiert. Um F_{10} als auch F_{11} vollständig zu faktorisieren, benutzte *Brent* die Faktorisierungsmethode, die auf der Theorie der elliptischen Kurven über $\mathbb{F}_p$ basiert (vgl. [36] bzw. [35]). Dieses Faktorisierungsverfahren (ECM) wurde von *H.W. Lenstra, Jr.* (vgl. [48]) erfunden. Der Grund weshalb F_{11} vor F_{10} vollständig faktorisiert werden konnte ist der, daß bei ECM der Schwierigkeitsgrad, eine Zahl vollständig zu faktorisieren von der Größe des zweitgrößten Primfaktors bestimmt wird. Der zweitgrößte Primfaktor von F_{11} mit 22 Dezimalstellen ist mit EMC viel leichter zu finden als der 40-stellige Primfaktor von F_{10}.

Bei F_{11} fand *Brent* die zwei kleineren Primfaktoren mit 21 bzw. 22 Dezimalstellen und deutete darauf hin, daß der übriggebliebene Kofaktor mit 564 Dezimalstellen wahrscheinlich prim wäre, was ein Jahr später von *Morain* bestätigt wurde.

Weiterhin fand mit dieser Faktorisierungsmethode *Crandall* 1991 zwei Primfaktoren von F_{13} (vgl. [6]). Einen weiteren Primfaktor von F_{13} ebenfalls mit ECM fanden *Brent, Crandall* und *Dilcher* 1995 sowie einen Primfaktor von F_{16} 1996 (vgl. [34]).

F_{14}, F_{20} und F_{22} sind die kleinsten und einzigen Fermat-Zahlen, von denen man weiß, daß sie zusammengesetzt sind, aber keinen einzigen Primfaktor kennt, und F_{24} mit 5050446 Dezimalstellen ist die kleinste Fermat-Zahl, von der man nicht weiß, ob sie prim oder zusammengesetzt ist. F_{23471} ist die größte Fermat-Zahl, von der man weiß, daß sie zusammengesetzt ist (vgl. Tabelle 2).

Außer den ersten fünf Fermat-Zahlen kennt man bis heute also keine weiteren Fermat-Primzahlen und man neigt zu der Vermutung, daß es überhaupt keine weitere Primzahl dieser Art gibt.

Die folgende Tabelle zeigt alle weiteren bis heute (aus mir zugänglicher Literatur) bekannten Primfaktoren von über 125 verschiedenen Fermat-Zahlen (vgl. auch Riesel [22], S. 384f.):

Tabelle 2: *Primfaktoren* $p = k \cdot 2^m + 1$ *der Fermat-Zahlen* $F_n = 2^{2^n} + 1$

n	k	m	Entdeckt von
12	7	14	Lucas, Pervouchine (1877)
	397	16	Western (1903)
	973	16	Western (1903)
	11613415	14	Hallyburton, Brillhart (1974)
	76668221074	14	Baillie (1986)
	Kofaktor: c_{1187}		
13	41365885	16	Hallyburton, Brillhart (1974)
	20323554055421	17	Crandall (1991)
	6872386635861	19	Crandall (1991)
	609485665932753836099	19	Brent et al (1995)
	Kofaktor: c_{2391}		
14	zusammengesetzt: c_{4933}		Selfridge, Hurwitz (1961)
15	579	21	Kraitchik (1925)
	17753925353	17	Gostin (1987)
	Kofaktor: c_{9840}		
16	1575	19	Selfridge (1953)
	180227048850079840107	20	Brent et al (1996)
	Kofaktor: c_{19694}		
17	59251857	19	Gostin (1980)
	Kofaktor: c_{39444}		
18	13	20	Western (1903)
	Kofaktor: c_{78906}		
19	33629	21	Riesel (1962)
	308385	21	Wrathall (1963)
20	zusammengesetzt		Buell, Young (1986)
21	534689	23	Wrathall (1963)
22	zusammengesetzt		Crandall et al (1993)
23	5	25	Pervouchine (1878)

Hierbei bedeutet c_r eine r-stellige Zahl, von der man weiß, daß sie nicht prim ist, "composite number".

6 Anhang

In Teil A werden mit *ARIBAS*-Funktion “factorlist” alle Primfaktoren einiger ausgesuchter Zahlenbeispiele in einem Vektor zusammengefaßt und ausgegeben.

Anschließend wird in Teil B von den gleichen Zahlenbeispielen die “Kettenbruchentwicklung ebenfalls mit Hilfe von *ARIBAS* (Funktion: “sqrtn2cfrac”) ausgerechnet und ausgegeben. Als Ergänzung habe ich auch die Periodenlänge L der Kettenbrüche angegeben.
Und schließlich werden in Teil C mit dem Faktorisierungs-Algorithmus von *Morrison* und *Brillhart* (*ARIBAS*-Funktion: “MB-factorize”) nach Primfaktoren einiger Zahlenbeispiele gesucht.

(Wie schon erwähnt, ist *ARIBAS* ein unter MS-DOS lauffähiger PASCAL-ähnlicher Multpräzisions-Interpreter, der auf einer Diskette zu Forster [8] erhältlich ist.)

7 Literaturverzeichnis

a) Bücher

1 A. Aigner: *Zahlentheorie*, de Gruyter, Berlin 1975

2 A. Baker: *Theory of Numbers*, Cambridge, University Press, 1984

3 D.M. Bressoud: *Factorization and Primality Testing*, Springer, New York, 1989

4 P. Bundschuh: *Einführung in die Zahlentheorie*, Springer, Berlin, 1988

5 H. Cohen: *A Course in Computational Algebraic Number Theory*, Springer, New York, 1993

6 R.E. Crandall: *Projects in Scientific Computation*, Springer, New York, 1996

7 L.E. Dickson: *History of the Theory of Numbers*, vol I (1919), reprint by Chelsea Books, New York, 1971 (speziell: Chapter XV)

8 O. Forster: *Algorithmische Zahlentheorie*, Vieweg, Braunschweig/Wiesbaden, 1996

9 R. Freud: *Grosse Augenblicke aus der Geschichte der Mathematik*, Bibliographisches Institut, 1990

10 P. Giblin: *Primes and Programming*, Cambridge, University Press, 1993

11 K.B. Gundlach: *Einführung in die Zahlentheorie*, Bibliographisches Institut, Mannheim, 1972

12 H. Hasse: *Vorlesungen über Zahlentheorie*, 2 Aufl., Springer, 1964

13 K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982

14 H. Koch: *Zahlentheorie*, Vieweg 1997

15 H.W. Lenstra, Jr., R. Tijdeman: *Computational Methods in Number Theory*, Part I, Math. Centre Tracts, # 154, Amsterdam, 1982

16 J.H. Loxton: *Number Theory and Cryptography*, Cambridge, University Press, 1990

17 W.A. Nikiforowski, L.F. Freimann: *Wegbereiter der neuen Mathematik*, MIR Moskau und VEB Leipzig, 1978

18 E. Pracht, K. Heidenreich: *Elementare Zahlentheorie*, Klett, Stuttgart, 1972

19 P. Ribenboim: *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979

20 P. Ribenboim: *The Book of Prime Number Records*, Springer, New York, 1988

21 P. Ribenboim: *The New Book of Prime Number Records*, Springer, New York, 1996

22 H. Riesel: *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1994

23 W. Scharlau, H. Opolka: *Von Fermat bis Minkowski*, Springer, Berlin, 1980

24 H. Scheid: *Einführung in die Zahlentheorie*, Klett, Stuttgart, 1972

25 H. Scheid: *Zahlentheorie*, Bibliographisches Institut Mannheim, 1991

26 D. Shanks: *Solved and Unsolved Problems in Number Theory*, Spartau Washington, 1962, 3rd edition by Chelsea Bronx New York, 1985

27 H. Wußing: *Vorlesungen zur Geschichte der Mathematik*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1979

b) Zeitschriften – Artikel

28 W.R. Alford, A. Granville, C. Pomerance: *There are Infinitely Many Carmichael Numbers*, Annals of Math., vol. 139 (1994), pp 703-722.

29 R.G. Ayoub, J.G. Huard, K.S. Williams: *Sarvadaman Chowla*, Notices Amer. Math. Soc. vol. 45 (1998), pp. 594-598.

30 R. Baillie: *New Primes of the Form* $k \cdot 2^n + 1$, Math. Comp. vol. 33 (1979), pp. 1333-1336.

31 D.J. Bernstein. *Detecting Perfect Primes in Essentially Linear Time*, Maht. Comp. vol. 67 (1998), p. 1253.

32 R.P. Brent: *Succinct Proofs of Primality for the Factors of Some Fermat Numbers*, Math. Comp. vol. 38 (1982), pp. 253-255.

33 R.P. Brent, J. Pollard: *Factorization of the Eigth Fermat Number*, Math. Comp. vol. 36 (1981), pp. 627-630.

34 R.P. Brent, R.E. Crandall, K. Dilcher: *Two New Factors of Fermat Numbers*, Report TR-CS-97-11, Australian National University, May 1997, 7 pp.

35 R.P. Brent: *Factorization of the Tenth and Eleventh Fermat Numbers*, Report TR-CS-96-02, Computer Sciences Laboratory, Australian National University, Canberra, Feb. 1996

36 R.P. Brent: *Factorization of the Tenth Fermat Number*, Math. Comp. (to appear)

37 J. Brillhart, J.L. Selfridge: *Some Factorizations of* $2^n \pm 1$ *and Related Results*, Math. Comp. vol. 21 (1967), pp. 87-96

38 S. Chowla, S.S. Pillai: *Periodic Simple Continued Fractions*, J. London Math. Soc. vol. 6 (1931), pp. 85-89

39 G.V. Cormack, H.C. Williams: *Some Very Large Primes of the Form* $k \cdot 2^m + 1$, Math. Comp. vol. 35 (1980), pp. 1419-1421

40 R. Crandall, J. Doenias, C. Norrie, J. Young: *The Twenty-second Fermat Number is Composite*, Math. Comp., vol. 64 (1995), pp. 863-869

41 R. Crandall, K. Dilcher, C. Pomerance: *A Search for Wieferich and Wilson Primes*, Math. Comp., vol. 66 (1997), pp. 433-449

42 B. Friedman, M. Hall: *Solutions to Problem 3707*, Amer. Math. Monthly vol. 44 (1937), pp. 397-400

43 G.B. Gostin, P.B. McLaughlin Jr.: *Six New Factors of Fermat Numbers*, Math. Comp. vol. 38 (1982), pp. 645-649

44 G.B. Gostin: *A Factor of F_{17}* , Math. Comp., vol. 35 (1980), pp. 975-976

45 G.B. Gostin: *New Factors of Fermat Numbers*, Math. Comp. vol. 64 (1995), pp. 393-395

46 J.C. Hallyburton, J. Brillhart: *Two New Factors of Fermat Numbers*, Math. Comp. vol. 29 (1975), pp. 109-112

47 W. Keller: *Factors of Fermat Numbers and Large Primes of the Form $k \cdot 2^n + 1$* , Math. Comp., vol. 41 (1983), pp. 661-673

48 H.W. Lenstra Jr.: *Factoring Integers with Elliptic Curves*, Annals Math. vol. 126 (1987), pp. 649-673

49 A.K. Lenstra, H.W. Lenstra Jr., M.S. Manasse, J.M. Pollard: *Factorization of the Ninth Fermat Number*, Math. Comp., vol. 61 (1993), pp. 319-349

50 J.C. Morehead: *Note on Fermat's Numbers*, Bull. Amer. Math. Soc. vol. 11 (1905). pp. 543-545

51 J.C. Morehead, A.E. Western: *Note on Fermat's Numbers*, Bull. Amer. Soc. vol. 16 (1909), pp. 1-6

52 M.A. Morrison, J. Brillhart: *A method of Factoring and the Factorization of F_7*, Math. Comp. vol. 29 (1975), pp. 183-208

53 M. Murra: *Methode und Anwendung des Number Field Sieve*, Diplomarbeit, Universität Bremen, 1998

54 G.A. Paxon: *The Compositiness of the Thirteenth Fermat Number*, Math. Comp. vol. 15 (1961), p. 420

55 C. Pomerance: *Cryptology and Computational Number Theory*, Proc. Sympos. Appl. Math. vol. 49, Amer. Math. Soc. Providence, RI, 1990

56 C. Pomerance: *A Tale of Two Sieves*, Notices of the Amer. Math. Soc. vol. 43 (1996) pp. 1473-1485

57 P. Ribenboim: *On the Square Factors of the Numbers of Fermat and Ferentinou-Nicolacopoulou*, Bull. Soc. Math. Grece (N.S.), vol. 20 (1979), pp. 81-92

58 H. Riesel: *A factor of the Fermat Number F_{19}*, Math. Comp. vol. 17 (1963), p. 458

59 R.M Robinson: *Mersenne and Fermat numbers*, Proc. Amer. Math. Soc. vol. 5 (1954), pp. 842-846

60 R.M. Robinson: *The Converse of Fermat's Theorem*, Amer. Math. Monthly, vol. 64 (1957), pp. 703-710

61 R.M. Robinson: *Factors of Fermat Numbers*, Math. Tables Aids Comput., vol. 11 (1957), pp. 21-22

62 R.M. Robinson: *A Report on Primes of the Form* $k \cdot 2^n + 1$ *and on Factors of Fermat Numbers*, Proc. Amer. Math. Soc. vol. 9 (1958), pp. 673-681

63 P. Seelhoff: *Die Auflösung grosser Zahlen in ihre Factoren*, Zeitschrift für Mathematik und Physik, vol. 31 (1886), pp. 166-174

64 J.L. Selfridge: *Factors of Fermat Numbers*, Math. Tables Aids Comp., vol. 7 (1953), pp. 274-275

65 J.L. Selfridge, A. Hurwitz: *Fermat Numbers and Mersenne Numbers*, Math. Comp., vol. 18 (1964), pp. 146-148

66 D.E. Shippee: *Four New Factors of Fermat Numbers*, Math. Comp., vol. 32 (1978), p. 941

67 R.G. Stanton, C. Sudler Jr., H.C. Williams: *An Upper Bound for the Period of the Simple Continued Fraction for* $\sqrt{D}$, Pacific J. Math., vol. 67 (1976), pp. 525-536

68 H. Suyama: *The Cofactor of* F_{15} *is Composite*, Abstracts Amer. Math. Soc., vol. 5 (1984), pp. 271-272

69 H.C. Williams: *How was* F_6 *factored?*, Math. Comp., vol. 61 (1993), pp. 463-474

70 C.P. Wrathall: *New Factors of Fermat Numbers*, Math. Comp., vol. 18 (1964), pp. 324-325

71 J. Young, D.A. Buell: *The Twentieth Fermat Number is Composite*, Math. Comp., vol. 50 (1988), pp. 261-263