Experimente zum Zeitaufwand der Primfaktorzerlegung

Ralph–Hardo Schulz

1. Einleitung

1.1 Zur früheren Rolle der Primzahlen.

Das Zerlegen einer Zahl in ihre Primfaktoren ist seit jeher eine Tätigkeit, die man im Schulunterricht zur Bestimmung von Teilern, gemeinsamen Teilern und gemeinsamen Vielfachen, zum Addieren (Hauptnennersuche) und Kürzen von Brüchen erlernt, aber außerhalb der Arithmetik kaum anwendet. So hatte auch das Interesse an der Zahlentheorie, der "Königin der Mathematik" von den (zum Teil zahlenmystischen) Anfängen bei Pythagoras, Eratosthenes, Diophant und Euklid an über die Verallgemeinerung der Teilbarkeit in der Algebra bis zu dem zeitgenössischen Beweis der Mordellvermutung (s. z.B. [Bun] p.177) durch G. Faltings (1983) und der Lösung des Fermat–Problems (s. z.B. [Bun] p.180) durch A. Wiles (1995) überwiegend akademische Gründe.

1.2 Primfaktorzerlegung und Falltüren in der Kryptologie

Ähnlich wie große Teile der Algebra "plötzlich" eine Anwendung in der Theorie der fehlerkorrigierenden Codes finden (s. [Schu_2]) und als mathematische Grundlage für die Technik des digitalen Fernsehens und der CD-Platte dienen, so ist die Zahlentheorie inzwischen als eines der Hilfsmittel der Kryptologie wichtig geworden, z. B. für die Sicherung von Zahlungsverkehr und Scheckkartensystemen, aber auch für die Authentifizierung von elektronisch übermittelten Dokumenten: Die zum Teil dafür verwandten öffentlichen Verschlüsselungssysteme, vorgeschlagen von Diffie und Hellman 1976, benötigen sogenannte **Falltür–Funktionen**, d. h. Funktionen, deren Funktionswerte sich auf einfache Weise berechnen lassen, bei denen aber der Schluß vom Funktionswert auf das zugehörige Argument ohne zusätzliche Information (dem geheimen Schlüssel) nur höchst rechenaufwendig zu erreichen ist.

Zu diesen Falltüren gehört (neben dem Potenzieren in endlichen Körpern) vermutlich die Bildung des Produkts zweier großer Primzahlen. Denn mit den bisher bekannten Verfahren ist die Primfaktorzerlegung von sehr großen Zahlen zeitaufwendig oder gar nicht möglich, s.u.. (Dies mag zunächst überraschen, aber man bedenke, daß die Zerlegung in Primfaktoren im Arithmetik–Unterricht der Schule meist mit kleinen Zahlen geübt wird.) Diese Falltüreigenschaft der Ganzzahl-Faktorisierung spielt eine große Rolle für das zur Zeit am meisten benutzte öffentliche Verschlüsselungssystem, das **RSA–Verfahren**, (s. z.B. [Bau], [Ber], [Beu], [Dew_2], [M], [Schu_1] §2C oder [Schu_2] 19.11), das 1978 von R. Rivest, A. Shamir und L. Adleman entwickelt worden ist.

Um die Sicherheit des RSA–Systems zu testen, veröffentlicht die Vertreiberfirma Zahlen, für deren Faktorisierung Preisgelder ausgesetzt sind; die kleinste Zahl unter diesen hat zur Zeit 140 Dezimalstellen (s. z.B. [Buc]). Trotz ausgefeilter Methoden (z.B. durch Verwendung elliptischer Kurven und neu entwickelter Siebe, s. z.B. [Buc]) gelingt es nur durch große Anstrengungen, 130 stellige Zahlen zu zerlegen. Fachleute erwarten, daß man in 5 Jahren 160–stellige Zahlen faktorisieren kann (s. [Buc]) und damit in die Größenordnung der zur Zeit im RSA–System verwendeten Produkte gelangt . Hingewiesen sei auch auf die Tatsache, daß sowohl die Experimente mit DERIVE als auch die erwähnte Einschätzung von ausgewiesenen Experten die Falltüreigenschaft zwar plausibel erscheinen lassen, diese aber nicht nachgewiesen werden kann. So könnte das Problem mit einem noch nicht entdeckten Algorithmus lösbar sein. Vielleicht schreitet ja auch die Hardware-Entwicklung , z.B. durch den projektierten Quantencomputer, soweit fort, daß die Faktorisierung bei den heute problematischen Fällen möglich wird. Es ist die Frage, ob sich die ganze Problematik dann lediglich in andere Größenordungen verlagert. Ebenfalls die Hilfe der Quantenmechanik beanspruchen völlig neu konzipierte Verfahren der "Quanten–Kryptographie", s. z.B. [BBE].

Es sei vermerkt, daß die Untersuchung einer Zahl daraufhin, ob sie Primzahl ist oder nicht (Primzahltest vgl. [Schu_1] §2E), wesentlich leichter ist als die Bestimmung der Faktoren im letzteren Fall. So geht es beim Wettlauf um die größte bekannte Primzahl um 65050– oder höher–stellige Zahlen (s. [Dew$_1$]).

1.3 Zielrichtung des vorliegenden Artikels

In vorliegendem Artikel geht es um die Vermittlung vereinfachter experimenteller Erfahrung zu der Falltüreneigenschaft der Produktbildung mit zwei (oder mehreren) Primzahlen. Dieser Gegenstand war, im Zusammenhang mit dem RSA–Verfahren, ein Teilthema bei einem Lehrerfortbildungskurs zum Thema Kryptologie, den der Autor zusammen mit OStRin I. Letzner und StD H. Witten [1] im Mai 1996 in Berlin veranstaltete. Zur Verfügung standen PC's mit dem Programm DERIVE. Die beobachteten qualitativen Phänomene sind aber unabhängig von den eingesetzten Programmpaketen und Rechnern, nur die quantitativen Größen variieren.

Da bei den Teilnehmern ein Defizit bei der Kenntnis der Definition von "Fermat–" bzw. "Mersenne–Zahlen" festzustellen war, schließen wir die Einleitung mit einem Exkurs über solche Zahlen, unter denen besonders viele Primzahlen vermutet wurden.

1.4 Fermat– und Mersenne–Zahlen

Fermat–Zahlen sind natürliche Zahlen von der Form $F_m = 2^{2^m} + 1$. Die Zahlen $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$ sind Primzahlen, weswegen Fermat (durch unvollständige Induktion) vermutete, daß alle Fermatzahlen Primzahlen sind. Aber schon Euler zeigte (1732), daß $F_5 = 641 \cdot 6700417$ ist. Bis F_{22} sind alle weiteren Fermatzahlen zusammengesetzt, aber die Faktorisierungen sind nicht alle bekannt (s. z.B. [R] p.87); hingewiesen sei hier auch auf den Artikel v. F. Fricker [F].

Mersenne–Zahlen sind definitionsgemäß von der Form $M_p = 2^p - 1$ mit Primzahl p. Z. B. sind $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ und $M_7 = 127$ Primzahlen, aber $M_{11} = 23 \cdot 89$ ist zusammengesetzt, ebenso M_{67} (siehe dazu die Schilderung in [F]). Eine Liste der bekannten Mersenne–Primzahlen findet man z.B. in [R] p. 94; die größte unter diesen ist M_{859433}.

[1] Herrn Witten danke ich für seine hilfreichen Hinweise zum Abfassen des vorliegenden Artikels.

Warum spielen gerade diese beiden Zahlentypen bei der Primzahlsuche eine Rolle? Eine besonders leichte Erzeugung vermutete man aus um 1 vermehrte oder verminderte Primzahlpotenzen; dies führte zur Betrachtung der Gleichung

$$q^d + 1 = p^r$$

mit Primzahlpotenz $q^d > 1$ und Primzahl p. Nun kann man zeigen (WALL), daß dann einer der folgenden Fälle vorliegen muß:

1. $d = 1$, $p = 2$, und q ist Mersenne–Primzahl
2. p ist Fermat–Primzahl, $r = 1$ und somit $q^d = p - 1 = 2^m$
3. $q^d = 8$, $p = 3$ und $r = 2$.

Im folgenden werden wir Tests mit Fermat– und Mersennezahlen gesondert vermerken, aber auch Zahlen der Form $2^d - 1$ mit d nicht prim betrachten.

1.5 Eine weitere klassische Möglichkeit, Primzahlen zu erzeugen, ist die Verwendung der Eulerschen Formel $m = n^2 + n + 41$, die u.a. für $n \leq 39$ Primzahlen liefert (s. z.B. [Sche]); auf diese Zahlen sind wir hier nicht weiter eingegangen.

1.6 Viele der Zahlen der Aufgabenstellung sind Produkte von Primfaktoren, die unter der Nebenbedingung etwa gleichgroßer vorgegebener Größen zufällig gewählt wurden. Für praktische Anwendungen wäre die Wahl der Faktoren nahe beieinander nicht optimal, da dann die Zerlegung von $n = p \cdot q$ in $n = (a + b)(a - b)$ (mit $a = (p + q)/2$ und $b = (p - q)/2$) durch die Betrachtung der Folge $a_k = a_0 + k$ für $k = 1, 2, 3, \ldots$ und Prüfen, ob $a_k^2 - n$ ein Quadrat ist, bei geeignetem Startwert a_0 schnell zum Ziel führen würde. Hingewiesen sei in diesem Zusammenhang auf das Beispiel der Zerlegung von Jevons'Zahl in [G].

2. Zeitaufwand für die Faktorisierung großer Zahlen

2.1 In Abbildung 1 geben wir einen Auszug aus dem Arbeitsblatt (mit kleinen Änderungen) an.

Aufgabenstellung.
Geben Sie (arbeitsteilig mit dem Programmpaket DERIVE) für folgende Zahlen die Primfaktorzerlegung an, und notieren Sie dabei die jeweils benötigte Rechenzeit.
Tragen Sie diese Rechenzeit in ein Diagramm ein, auf dessen Abszisse (x–Achse) die Stellenzahl und auf dessen Ordinate (y–Achse) die Rechenzeit skaliert ist!

Zahl	Faktorisierung	Rechenzeit	Stellenzahl
Beispiel:			
138909787	$= 11783 \cdot 11789$	0.9 sec	9 St.
Aufgaben:			
5964848081	=	......	......
8616460799	=	......	......
13141611137	=	......	......
⋮			

Abb.1 : Auszug aus dem Arbeitsblatt

Aus Platzgründen geben wir hier die weiteren zu faktorisierenden Zahlen an

17543877193, 241873694197, 4156338464051, 18128486155487, 191427922718503, 191427922719503, 1054054986561173, 5210760312902717, 31901620774254383, 68442389367182561, 965521343020615207, 1111111111111111111, 4160426670634335197, 43428084786416441631, 415758465533848642967, 316362908763458525001406154038726382279, 11111111111111111111111111111111111111111111, 465235439986679108204139705633885130899652358311 .

Einige Fermat–Zahlen

$2^{2^4} + 1\ ,\quad 2^{2^5} + 1\ ,\quad 2^{2^6} + 1,\quad 2^{2^7} + 1$

Einige Mersenne-Zahlen und Ähnliche

$2^{30}-1,\quad 2^{31}-1,\quad 2^{60}-1,\quad 2^{61}-1,\quad 2^{89}-1,\quad 2^{107}-1,\quad 2^{127}-1,$

$2^{140}-1,\quad 2^{147}-1,\quad 2^{148}-1,\quad 2^{149}-1,\quad 2^{151}-1,\quad 2^{154}-1$

$2^{155}-1,\quad 2^{157}-1,\quad 2^{257}-1$

2.2 Lösungen

Da das Programmpaket DERIVE weitgehend selbsterklärend ist, braucht außer den Anweisungen zur Installation kaum weitere Hilfestellung gegeben werden. Hier trotzdem einige Hinweise: Man beginnt mit dem COMMAND: $\boxed{\text{AUTHOR}}$ in der Befehlsliste unten, gibt für die $\boxed{\text{AUTHOR expression}}$ die zu zerlegende Zahl ein, danach die COMMANDS: $\boxed{\text{Factor}}$ und $\boxed{\text{Factor expression} \sharp 1}$ und erhält unter Nr. 2 die Faktoren sowie in der vorletzten Zeile die Rechenzeit. Für die erste Faktorisierung ergibt sich z. B. die Anzeige gemäß Abbildung 2. Bei den Fermat- und Mersenne-Zahlen benutzt man zur Berechnung der Zahl zuvor noch den "Simplify" – Befehl. Falls der Faktorisierungs–Vorgang zu lange dauert, läßt er sich mit der "Esc"–Taste der Tastatur abbrechen. (Vgl. auch [KBG] p. 366 – 368 und [Sche] !)

Am Ende des Experiments wurden Lösungsblätter gemäß Abbildungen 3 bis 6 (hier ebenfalls geringfügig geändert) verteilt.

2.3 Graphische Darstellung des Zeitaufwands

Die in der Aufgabenstellung geforderte graphische Darstellung sollte in etwa die Meßwerte wiee in Abbildung 7 enthalten. Die eingezeichneten Kurven sollen die kritische Zone beschreiben; sie approximieren eine im Argument diskrete, keine kontinuierliche Situation; sie sind also nur Veranschauungshilfen.

2.4 Weitere Kommentare

Wie schon erwähnt, hängt der Zeitaufwand quantitativ von dem verwendeten PC und dem verwendeten Programm ab. Wir haben aber allen Anlaß zu der Vermutung, daß die Beobachtung bei festem Rechner und üblichem Programm qualitativ gleiche Phänomene aufweist. Auch bei den zur Zeit modernen Algorithmen verdoppelt sich die Rechenzeit bei Übergang von 130 zu 133 Dezimalstellen (s. [Buc], p. 88 unter "Perspektiven").

Warum Fermat– und Mersenne–Zahlen den Anstieg der Rechenzeit erst bei vergleichsweise höherer Stellenzahl aufweisen, ist ein Phänomen, für das wir nur die Erklärung haben, daß bei den untersuchten Zahlen meist auch sehr kleine Primteiler vorkommen. Bei den anderen Zahlenbeispielen haben wir meist ungefähr gleich große Faktoren gewählt, um die "Randzone" (schraffiert) experimentell zu bestimmen; natürlich gibt es immer Zahlen höherer Stellenzahl, deren Faktorisierung wesentlich schneller geht.

Sicher gibt es insgesamt noch weiteren Erklärungsbedarf und auch Erklärungsmöglichkeiten. Für Hinweise diesbezüglich sind wir dankbar.

3. Literaturhinweise

[Bau] Bauer, F. L.: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. Springer Verlag, Berlin etc. 1995.

[BBE] Bennett, C.H., G. Brassard und A.K. Ekert: Quanten – Kryptographie. Spektrum der Wissenschaft, Dez. 1992 p. 96 – 104.

[Ber] Berendt, G.: Elemente der Kryptologie. In: Math. Aspekte der Angewandten Informatik. R.-H. Schulz (Hrsg.), BI Wissenschaftsverlag, Mannheim 1994, p. 128-146.

[Beu] Beutelspacher, A.: Kryptologie, Vieweg Verlag, Braunschweig 1987, 1994[4].

[Buc] Buchmann, J.: Faktorisierung großer Zahlen, Spektrum der Wissenschaft, Sept. 1996, 80 – 88.

[Bun] Bundschuh, P.: Einführung in die Zahlentheorie, Springer Verlag, Berlin–Heidelberg–New York, 1992.

[Dew$_1$] Dewdney, A.K.: Primzahlwäsche. In: Computer Kurzweil 2, Spektrum Akad. Verlag, Heidelberg 1992, p. 175 – 178.

[Dew$_2$] Dewdney, A. K.: Moderne Verschlüsselungssysteme. In: Computer Kurzweil 2, Spektrum Akad. Verlag, Heidelberg 1992, p. 183 – 187.

[F] Fricker, F.: Neue Rekordfaktorisierung, Spektrum der Wissenschaft, Nov. 1990, p. 38 – 42.

[G] Golomb, S.W.: On factoring Jevons' number. Cryptologia **20**/3 (1996) p. 243–246.

[KBG]Koepf, W., A.Ben–Israel und B.Gilbert: Mathematik mit Derive, Vieweg V., Braunschweig/Wiesbaden 1993.

[M] Maurer, U.: Kryptologie: eine neuartige Anwendung der Mathematik. El. Math. **50** (1995) p. 89 – 106.

[R] Ribenboim, P.: The new book of prime number records, Springer Verlag, New York 1996^3.

[Sche] Scheu, G.: Entdeckungen in der Menge der Primzahlen mit DERIVE. Praxis der Math. PM 3/**34** (1992) p. 119 – 122.

[Schu$_1$] Schulz, R. -H.: Primzahlen in öffentlichen Chiffrierverfahren. Mathematik lehren **61** (1993) 56 – 64.

[Schu$_2$] Schulz, R. -H.: Codierungstheorie. Eine Einführung. Vieweg Verlag, Braunschweig/Wiesbaden 1991, Kap. IV: Kryptographie.

Adresse des Autors:

Prof.Dr.Ralph-Hardo Schulz
2. Math. Inst. der Freien Universität
Arnimallee 3
D-14195 Berlin

E-mail: schulz@math.fu-berlin.de
Fax (Institut): 030-838-75404

1: 138909787

2: 11783 11789

COMMAND: Author Build Calculus Declare Expand Factor Help Jump soLve Manage
Options Plot Quit Remove Simplify Transfer moVe Window approX

Compute time: 0.9 seconds

Fctr (1) Free: 95% Derive Algebra

Abb. 2 : Anzeige auf den Display nach Lösung der ersten Teilaufgabe

Einige große Zahlen und ihre Faktorisierung

(mit Rechenzeit auf Compaq 386/20 e mit Derive Version 2.08)

Zahl	Faktorisierung	Zeitaufwand	Stellenzahl
138909787	$=11783 \cdot 11789$	0.9 sec	9 St.
5964848081	$=5964848081$	0.9 sec	10 St.
8616460799	$=89681 \cdot 96079$	0.1 sec	10 St.[2]
13141611137	$=269 \cdot 2543 \cdot 19211$	0.9 sec	11 St.
17543877193	$=52579 \cdot 333667$	0.7 sec	11 St.
241873694197	$=15619 \cdot 15485863$	0.2 sec	12 St.
4156338464051	$=2038717 \cdot 2038703$	2.9 sec	13 St.
18128486155487	$=4257749 \cdot 4257763$	4.5 sec	14 St.
191427922718503	$=131 \cdot 1461281852813$	0.9 sec	15 St.
191427922719503	$=13835747 \cdot 13835749$	7.3 sec	15 St.
1054054986561173	$=32466199 \cdot 32466227$	14,4 sec	16 St.
5210760312902717	$=32466227 \cdot 160497871$	14.3 sec	16 St.
31901620774254383	$=32466227 \cdot 982609429$	15.8 sec	17 St.
68442389367182561	$=15485863 \cdot 4419669047$	15.1 sec	17 St.
965521343020615207	$=982609429 \cdot 982609483$	131 sec	18 St.
1111111111111111111	$=1111111111111111111$	0.2 sec	19 St.
4160426670634335197	$=2039712397 \cdot 2039712401$	111.3 sec	19 St.
4342808478641644163	$=982609429 \cdot 4419669047$	129.7 sec	19 St.
415758465533848642967	$=11110693267 \cdot 37419669101$	228.9 sec	21 St.

Abb. 3 : 1. Lösungsblatt

[2] Diese Zahl wurde 1873 von JEVONS angegeben, der die Falltüreigenschaft der Produktbildung großer Zahlen antizipierte , aber fälschlicherweise glaubte, diese Zahl könne von niemandem faktorisiert werden, s. [G]. Hier liegen die Faktoren so nahe beieinander, daß auch mit den damaligen Hilfsmitteln eine Zerlegung möglich gewesen wäre, siehe 1.6 oben oder bei [G].

3163629087634585250014061540387263822 79			
	=3163629087634585250014061540387263822 79	1 sec	39 St.
11111111111111111111111111111111111111111111111			
	$=35121409 \cdot 3163629087634585250014061540387263822 79$	23.5 sec	47 St.
465235439986679108204139705633885130899652358311 = ???			48 St.
(Anmerkung: $=2305843009213693951 \cdot 201763709900322803748657942361$)			

Fermat-Zahlen

$2^{2^4}+1=65537$	=65537	"0.0" sec	5 St.
$2^{2^5}+1=4294967297$	$=641 \cdot 6700417$	0.2 sec	10 St.
$2^{2^6}+1=18446744073709551617$	$= 274177 \cdot 67280421310721$	7.3 sec	20 St.
$2^{2^7}+1=340282366920938463463374607431768211457 \approx 3,4 \cdot 10^{38}$		???	39 St.
(Anmerkung $=59649589127497217 \cdot 5704689200685129054721$)			

Mersenne-Zahlen und Ähnliche

$2^{30}-1=1073741823=3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$		0.0 sec	10 St.
$2^{31}-1$ =2147483647 =2147483647 (Euler)		0.2 sec	10 St.
$2^{60}-1=$ 1152921504606846975			
	$=3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$	0.1 sec	19 St.

Abb. 4 : 2. Lösungsblatt

$2^{61}-1 = 2305843009213693951 =$	2305843009213693951 (Pervushin)	0.3 sec	19 St.
$2^{89}-1 = 618970019642690137449562111 =$	$618970019642690137449562111$ (Powers)	0.4 sec	27 St.
$2^{107}-1 = 162259276829213363391578010288127 =$	$162259276829213363391578010288127$ (Fauquembergue)	0.5 sec	33 St.
$2^{127}-1 = 170141183460469231731687303715884105727 =$	$170141183460469231731687303715884105727$ (Lucas)	1.2 sec	39 St.
$2^{140}-1 = 1393796574908163946345982392040522594123775 =$	$3 \cdot 5^2 \cdot 11 \cdot 29 \cdot 31 \cdot 41 \cdot 43 \cdot 71 \cdot 113 \cdot 127 \cdot 281 \cdot 86171 \cdot 122921 \cdot 7416361 \cdot 47392381$	7.6 sec	43 St.
$2^{147}-1 = 178405961588244985132285746181186892047843327 =$	$7^3 \cdot 127 \cdot 337 \cdot 4432676798593 \cdot 2741672362528725535068727$	???	45 St.
$2^{148}-1 = 356811923176489970264571492362373784095686655 =$	$3 \cdot 5 \cdot 149 \cdot 223 \cdot 593 \cdot 1777 \cdot 25781083 \cdot 184481113 \cdot 231769777 \cdot 616318177$	82.9 sec	45 St.
$2^{149}-1 = 713623846352979940529142984724747568191373311$	(Anmerkung: Keine Primzahl)	???	45 St.
$2^{151}-1 = 2854495385411919762116571938898990272765493247 =$	$18121 \cdot 55871 \cdot 165799 \cdot 2332951 \cdot 7289088383388253664437433$	11.8 sec	46 St.
$2^{154}-1 = 22835963083295358096932575511191922182123945983 =$	$3 \cdot 23 \cdot 43 \cdot 89 \cdot 127 \cdot 617 \cdot 683 \cdot 78233 \cdot 35532364099 \cdot 581283643249112959$	157.6 sec	47 St.

Abb. 5 : 3. Lösungsblatt

$2^{155} - 1 = 45671926166590716193865151022383844364247891967=$

$31^2 \cdot 311 \cdot 11471 \cdot 73471 \cdot 2147483647 \cdot 4649919401 \cdot 1815820981351$ 171.8 sec 47 St.

$2^{157} - 1 = 182687704666362864775460604089535377456991567871=$??? 48 St.

(Anmerkung: Keine Primzahl)

$2^{257} - 1 =$

$231584178474632390847141970017375815706539969331281128078915168015826259279871$

$\approx 2,3 \cdot 10^{74}$??? (Anmerkung: Keine Primzahl)

Kommentare:

Der Anstieg der Rechenzeit ist etwa exponentiell; ohne die verschiedenen möglichen Verfahren im einzelnen zu untersuchen, können wir zitieren (s. Bauer: Kryptologie, §11.2): Es gibt einen Algorithmus zur Zerlegung einer Zahl n in Primfaktoren, dessen Operationen-Anzahl asymptotisch in der Größenordnung von $e^{\sqrt{ln(n) ln(ln(n))}}$ liegt [3].

U.a. bei folgenden Sachverhalten kann die Rechenzeit jedoch wesentlich kürzer sein:

- n ist Primzahl
- n enthält einen oder mehrere kleine Faktoren
- n ist Produkt zweier Zahlen ungefähr gleicher Stellenzahl
- n ist Fermat'sche oder Mersenne'sche Zahl

Abb. 6 : 4. Lösungsblatt

[3] Nach [M] ist die Laufzeit des asymptotisch schnellsten bekannten Algorithmus $c_1 e^{c_2 n^{1/3} (\ln(n))^{2/3}}$. Er stammt von LENSTRA, POLLARD und anderen.

Abb. 7 : Graphische Darstellung des für die Faktorisierungen benötigten Zeitaufwands (in Abhängigkeit von der Stellenzahl)