Die nun folgenden Faktorisierungen wurden durchgeführt auf einem **AMD Ryzen 9 5900X**

Programme zur Faktorisierung mit Ermittlung der Berechnungszeit

1) CrypTool2 ; GUI (max.Stellenzahl = 100)

2) Yafu-x64 2.10 (Konsolenprogramm; C++; Ben Buhrow) ; Aufruf z.B.: yafu-x64 factor(1001)

3) alpertron programs (Dario Alpern; verwendet Elliptische Kurven - läuft im Browser; C++)

4) wxMaxima(CAS; GUI) ; Aufruf z.B. factor(576);

5) PARI/GP 2.15.5 (Konsolenprogramm von Karim Belabas)) ; Aufruf z.B. factor(1001);

6) Tilman Neumann: JavaMathLibrary ; Aufruf: PSIQS_U (bzw. PSIQS bzw. SIQS)

7) jLangZahlToolDecGUI www.k-achilles.de/java.html (jar executable GUI von Ac)

8) factor von Kay Schönberger (von der Console aus aufrufbar, z.B. factor 1001)

ct2: meint CrypTool2 (Quadratisches Sieb; 12 Prozessorkerne ; 24 Threads)
Yafu: meint yafu-x64 , V2.08 . yafu/s meint Verwendung von siqs(..)
max: meint wxMaxima
pari: meint PARI/GP
Til: meint Tilman Neumann ; Til/P für PSIQS Til/S für SIQS
rho: bzw. brent bzw. fmt(Fermat) bzw. Leh(Lehman) bzw. Ac: meint meine Teilprogramme von ***jLangzahlToolDecGUI*** (mein Java-Programm).
Schö: meint factor von K.Schönberger

Einige **zerlegbare** Mersennezahlen Mn:

Zerlegung der Mersennezahlen von M4 bis M200:

M4 = 15 = 3·5
M6 = 63 = 3·3·7
M8 = 255 = 3·5·17
M9 = 511 = 7·73
M10 = 1023 = 3·11·31
M11 = 2047 = 23·89
M12 = 4095 = 3·3·5·7·13
M14 = 16383 = 3·43·127
M15 = 32767 = 7·31·151
M16 = 65535 = 3·5·17·257
M18 = 262143 = 3·3·3·7·19·73
M20 = 1048575 = 3·5·5·11·31·41
M21 = 2097151 = 7·7·127·337
M22 = 4194303 = 3·23·89·683
M23 = 8388607 = 47·178481
M24 = 16777215 = 3·3·5·7·13·17·241
M25 = 33554431 = 31·601·1801
M26 = 67108863 = 3·2731·8191
M27 = 134217727 = 7·73·262657
M28 = 268435455 = 3·5·29·43·113·127
M29 = 536870911 = 233·1103·2089
M30 = 1073741823 = 3·3·7·11·31·151·331
M32 = 4294967295 = 3·5·17·257·65537
M33 = 8589934591 = 7·23·89·599479
M34 = 17179869183 = 3·43691·131071
M35 = 34359738367 = 31·71·127·122921
M36 = 68719476735 = 3·3·3·5·7·13·19·37·73·109
M37 = 137438953471 = 223·616318177
M38 = 274877906943 = 3·174763·524287
M39 = 549755813887 = 7·79·8191·121369
M40 = 1099511627775 = 3·5·5·11·17·31·41·61681
M41 = 2199023255551 = 13367·164511353
M42 = 4398046511103 = 3·3·7·7·43·127·337·5419
M43 = 8796093022207 = 431·9719·2099863
M44 = 17592186044415 = 3·5·23·89·397·683·2113
M45 = 35184372088831 = 7·31·73·151·631·23311
M46 = 70368744177663 = 3·47·178481·2796203
M47 = 140737488355327 = 2351·4513·13264529
M48 = 281474976710655 = 3·3·5·7·13·17·97·241·257·673
M49 = 562949953421311 = 127·4432676798593
M50 = 1125899906842623 = 3·11·31·251·601·1801·4051
M51 = 2251799813685247 = 7·103·2143·11119·131071
M52 = 4503599627370495 = 3·5·53·157·1613·2731·8191
M53 = 9007199254740991 = 6361·69431·20394401
M54 = 18014398509481983 = 3·3·3·3·7·19·73·87211·262657
M55 = 36028797018963967 = 23·31·89·881·3191·201961
M56 = 72057594037927935 = 3·5·17·29·43·113·127·15790321
M57 = 144115188075855871 = 7·32377·524287·1212847
M58 = 288230376151711743 = 3·59·233·1103·2089·3033169
M59 = 576460752303423487 = 179951·3203431780337
M60 = 1152921504606846975 = 3·3·5·5·7·11·13·31·41·61·151·331·1321
M62 = 4611686018427387903 = 3·715827883·2147483647
M63 = 9223372036854775807 = 7·7·73·127·337·92737·649657
M64 = 18446744073709551615 = 3·5·17·257·641·65537·6700417
M65 = 36893488147419103231 = 31·8191·145295143558111
M66 = 73786976294838206463 = 3·3·7·23·67·89·683·20857·599479
M67 = 147573952589676412927 = 193707721·761838257287
M68 = 295147905179352825855 = 3·5·137·953·26317·43691·131071
M69 = 590295810358705651711 = 7·47·178481·10052678938039
M70 = 1180591620717411303423 = 3·11·31·43·71·127·281·86171·122921
M71 = 2361183241434822606847 = 228479·48544121·212885833
M72 = 4722366482869645213695 = 3·3·3·5·7·13·17·19·37·73·109·241·433·38737
M73 = 9444732965739290427391 = 439·2298041·9361973132609
M74 = 18889465931478580854783 = 3·223·1777·25781083·616318177
M75 = 37778931862957161709567 = 7·31·151·601·1801·100801·10567201
M76 = 75557863725914323419135 = 3·5·229·457·174763·524287·525313
M77 = 151115727451828646838271 = 23·89·127·581283643249112959
M78 = 302231454903657293676543 = 3·3·7·79·2731·8191·121369·22366891
M79 = 604462909807314587353087 = 2687·202029703·1113491139767
M80 = 1208925819614629174706175 = 3·5·5·11·17·31·41·257·61681·4278255361
M81 = 2417851639229258349412351 = 7·73·2593·71119·262657·97685839
M82 = 4835703278458516698824703 = 3·83·13367·164511353·8831418697

M83 = 9671406556917033397649407 = 167·579126141132756490877 21
M84 = 19342813113834066795298815 = 3·3·5·7·7·13·29·43·113·127·337·1429·5419·14449
M85 = 38685626227668133590597631 = 31·131071·9520972806333758431
M86 = 77371252455336267181195263 = 3·431·9719·2099863·2932031007403
M87 = 15474250491067253436239052 7 = 7·233·1103·2089·4177·9857737155463
M88 = 30948500982134506872478105 5 = 3·5·17·23·89·353·397·683·2113·2931542417
M90 = 12379400392853802748991242 23 = 3·3·3·7·11·19·31·73·151·331·631·23311·18837001
M91 = 24758800785707605497982484 47 = 127·911·8191·112901153·23140471537
M92 = 49517601571415210995964968 95 = 3·5·47·277·1013·1657·30269·178481·2796203
M93 = 99035203142830421991929937 91 = 7·2147483647·658812288653553079
M94 = 19807040628566084398385987583 = 3·283·2351·4513·13264529·165768537521
M95 = 39614081257132168796771975167 = 31·191·524287·420778751·30327152671
M96 = 79228162514264337593543950335 = 3·3·5·7·13·17·97·193·241·257·673·65537·22253377
M97 = 15845632502852867518708790067 1 = 11447·13842607235828485645766393
M98 = 31691265005705735037417580134 3 = 3·43·127·43639531272974432676798593
M99 = 63382530011411470074835160268 7 = 7·23·73·89·199·153649·599479·33057806959
M100 = 12676506002282294014967032053 75 = 3·5·5·5·11·31·41·101·251·601·1801·4051·8101·268501
M101 = 25353012004564588029934064107 51 = 7432339208719·341117531003194129
M102 = 50706024009129176059868128215 03 = 3·3·7·103·307·2143·2857·6529·11119·43691·131071
M103 = 10141204801825835211973625643 007 = 2550183799·3976656429941438590393
M104 = 20282409603651670423947251286 015 = 3·5·17·53·157·1613·2731·8191·858001·308761441
M105 = 40564819207303340847894502572 031 = 7·7·31·71·127·151·337·29191·106681·122921·152041
M106 = 81129638414606681695789005144 063 = 3·107·6361·69431·20394401·28059810762433
M108 = 32451855365842672678315602057 6255 = 3·3·3·3·5·7·13·19·37·73·109·87211·246241·262657·279073
M109 = 64903710731685345356631204115 2511 = 745988807·870035986098720987332873
M110 = 12980742146337069071326240823 05023 = 3·11·11·23·31·89·683·881·2971·3191·201961·48912491
M111 = 25961484292674138142652481646 10047 = 7·223·321679·26295457·319020217·616318177
M112 = 51922968585348276285304963292 20095 = 3·5·17·29·43·113·127·257·5153·15790321·54410972897
M113 = 10384593717069655257060992658 440191 = 3391·23279·65993·1868569·1066818132868207
M114 = 20769187434139310514121985316 880383 = 3·3·7·571·32377·174763·524287·1212847·160465489
M115 = 41538374868278621028243970633 760767 = 31·47·14951·178481·4036961·2646507710984041
M116 = 83076749736557242056487941267 521535 = 3·5·59·233·1103·2089·3033169·107367629·536903681
M117 = 16615349947311448411297588253 5043071 = 7·73·79·937·6553·8191·86113·121369·7830118297
M118 = 33230699894622896822595176507 0086143 = 3·2833·37171·179951·1824726041·3203431780337
M119 = 66461399789245793645190353014 0172287 = 127·239·20231·131071·62983048367·131105292137
M120 = 13292279957849158729038070602 80344575 =
3·3·5·5·7·11·13·17·31·41·61·151·241·331·1321·61681·4562284561
M121 = 26584559915698317458076141205 60689151 = 23·89·727·178639387836316422785827 0210279
M122 = 53169119831396634916152282411 21378303 = 3·768614336404564651·2305843009213693951
M123 = 10633823966279326983230456482 242756607 = 7·13367·3887047·164511353·177722253954175633
M124 = 21267647932558653966460912964 485513215 = 3·5·5581·8681·49477·384773·715827883·2147483647
M125 = 42535295865117307932921825928 971026431 = 31·601·1801·269089806001·4710883168879506001
M126 = 85070591730234615865843651857 942052863 =
3·3·3·7·7·19·43·73·127·337·5419·92737·649657·77158673929
M128 = 34028236692093846346337460743 1768211455 = 3·5·17·257·641·65537·274177·6700417·67280421310721
M129 = 68056473384187692692674921486 3536422911 = 7·431·9719·2099863·1105303606504929475345963 9
M130 = 13611294676837538538534984297 27072845823 =
3·11·31·131·2731·8191·409891·7623851·145295143558111
M131 = 27222589353675077077069968594 54145691647 = 263·1035079443105516238671861923746823456 9
M132 = 54445178707350154154139937189 08291383295 =
3·3·5·7·13·23·67·89·397·683·2113·20857·312709·599479·4327489
M133 = 10889035741470030830827987437 816582766591 = 127·524287·16353722085272539885143432572095 9
M134 = 21778071482940061661655974875 633165533183 = 3·7327657·193707721·761838257287·6713103182899
M135 = 43556142965880123323311949751 266331066367 =
7·31·73·151·271·631·23311·262657·348031·49971617830801
M136 = 87112285931760246646623899502 532662132735 =
3·5·17·17·137·953·26317·43691·131071·354689·2879347902817
M137 = 17422457186352049329324779900 5065324265471 =
32032215596496435569·543904218360020429015 9 42 Stellen pari: 0,05s Yafu: 0,3s
M138 = 34844914372704098658649559801 0130648530943 =
3·3·7·47·139·178481·2796203·168749965921·10052678938039
M139 = 69689828745408197317299119602 0261297061887 = 5625767248687·123876132205208335762278423601
M140 = 13937965749081639463459823920 40522594123775 =
3·5·5·11·29·31·41·43·71·113·127·281·86171·122921·7416361·47392381
M141 = 27875931498163278926919647840 81045188247551 =
7·2351·4513·13264529·4375578271·646675035253258729
M142 = 55751862996326557853839295681 62090376495103 =
3·228479·48544121·56409643·212885833·13952598148481
M143 = 11150372599265311570767859136 324180752990207 =
23·89·8191·724153·158822951431·5782172113400990737
M144 = 22300745198530623141535718272 648361505980415 =
3·3·3·5·7·13·17·19·37·73·97·109·241·257·433·577·673·38737·487824887233
M145 = 44601490397061246283071436545 296723011960831 =
31·233·1103·2089·26798951577838628146900274941449 91
M146 = 89202980794122492566142873090 593446023921663 =
3·439·1753·2298041·9361973132609·1795918038741070627

M147 = 178405961588244985132285746181186892047843327 =
7·7·7·127·337·4432676798593·27416723625287255350687 27 45 Stellen brent: 0,2s
M148 = 35681192317648997026457149236237378409568665 5 =
3·5·149·223·593·1777·25781083·184481113·231769777·616318177
M149 = 71362384635297994052914298472474756819137331 1 =
86656268566282183151· 82351093366908467239861 61 45 Stellen pari: 0,1s
M150 = 14272476927059598810582859694494951363827466 23 =
3·3·7·11·31·151·251·331·601·1801·4051·100801·10567201·1133836730401
M151 = 28544953854119197621165719388989902727654932 47 =
18121·55871·165799·2332951·728908838338825366443743 33
M152 = 57089907708238395242331438777979805455309864 95 =
3·5·17·229·457·1217·148961·174763·524287·525313·24517014940753
M153 = 11417981541647679048466287755595961091061972 99 1 =
7·73·103·919·2143·11119·131071·75582488424179347083438319
M154 = 22835963083295358096932575511191922182123945 98 3 =
3·23·43·89·127·617·683·78233·35532364099·581283643249112959
M155 = 45671926166590716193865151022383844364247891 96 7 =
31·31·311·11471·73471·2147483647·4649919401·18158209813151
M156 = 91343852333181432387730302044767688728495783 93 5 =
3·3·5·7·13·13·53·79·157·313·1249·1613·2731·3121·8191·21841·121369·22366891
M157 = 18268770466636286477546060408953537745699156787 1 =
852133201·60726444167·1654058017289·2134387368610417 48 Stellen brent: 0,4s
M158 = 36537540933272572955092120817907075491398313574 3 =
3·2687·202029703·1113491139767·201487636602438195784363
M159 = 73075081866545145910184241635814150982796627148 7 =
7·6361·6679·69431·13960201·20394401·540701761·229890275929
M160 = 14615016373309029182036848327162830195659325429 75 =
3·5·5·11·17·31·41·257·61681·65537·414721·4278255361·44479210368001
M161 = 29230032746618058364073696654325660393118650859 51 =
47·127·1289·178481·3188767·45076044553·14808607715315782481
M162 = 58460065493236116728147393308651320786237301719 03 =
3·3·3·3·3·7·19·73·163·2593·71119·87211·135433·262657·97685839·272010961
M163 = 11692013098647223345629478661730264157247460343807 =
150287·704161·110211473·27669118297·36230454570129675721
M164 = 23384026197294446691258957323460528314494920687615 =
3·5·83·10169·13367·181549·12112549·43249589·164511353·8831418697
M165 = 46768052394588893382517914646921056628989841375231 =
7·23·31·89·151·881·3191·201961·599479·2048568835297380486760231
M166 = 93536104789177786765035829293842113257979682750463 =
3·167·499·1163·2657·155377·13455809771·57912614113275649087721
M167 = 18707220957835557353007165858768422651595936550092 7 =
2349023·7963830476685650737777861629608744849069564 9
M168 = 37414441915671114706014331717536845303191873100185 5 =
3·3·5·7·7·13·17·29·43·113·127·241·337·1429·3361·5419·14449·15790321·88959882481
M169 = 74828883831342229412028663435073690606383746200371 1 =
4057·8191·6740339310641·33407622839523953295063270230 33
M170 = 14965776766268445882405732687014738121276749240074 23 =
3·11·31·43691·131071·9520972806333758431·26831423036065352611
M171 = 29931553532536891764811465374029476242553498480148 47 =
7·73·32377·524287·1212847·93507247·30426456347925413120378 47
M172 = 59863107065073783529622930748058952485106996960296 95 =
3·5·173·431·9719·101653·500177·2099863·1759217765581·2932031007403
M173 = 11972621413014756705924586149611790497021399392059391 =
730753·1505447·70084436712553223·155285743288572277679887
M174 = 23945242826029513411849172299223580994042798784118783 =
3·3·7·59·233·1103·2089·4177·3033169·9857737155463·96076791871613611
M175 = 47890485652059026823698344598447161988085597568237567 =
31·71·127·601·1801·39551·122921·60816001·535347624791488552837151
M176 = 95780971304118053647396689196894323976171195136475135 =
3·5·17·23·89·257·353·397·683·2113·229153·119782433·2931542417·43872038849
M177 = 19156194260823610729479337839378864795234239027295 02 71 =
7·179951·184081·27989941729·3203431780337·92136240845359890 31
M178 = 38312388521647221458958675678757729590468478054590 05 43 =
3·179·62020897·18584774046020617·6189700196426901374495621 11
M179 = 76624777043294442917917351357515459180936956109180 10 87 =
359·1433·14894591093600398664569401970954337216649519991 21
M180 = 15324955408658888583583470271503091836187391221836021 75 =
$3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 109 \cdot 151 \cdot 181 \cdot 331 \cdot 631 \cdot 1321 \cdot 23311 \cdot 54001 \cdot 18837001 \cdot 29247661$
M181 = 30649910817317777167166940543006183672374782443672043 51 =
43441·1164193·7648337·79238710972852956253446476657646726 71
M182 = 61299821634635554334333881086012367344749564887344087 03 =
3·43·127·911·2731·8191·224771·1210483·112901153·23140471537·25829691707
M183 = 12259964326927110866866776217202473468949912977468817407 =
7·367·55633·2305843009213693951·37201708625305146303973352041
M184 = 24519928653854221733733552434404946937899825954937634815 =
3·5·17·47·277·1013·1657·30269·178481·2796203·29128000924361888821155864 1

M185 = 490398573077084434674671048688098938757996519098752696 31 =
31·223·616318177·1587855697992791·724880859928576000115275564 1
M186 = 980797146154168869349342097376197877515993038197505392 63 =
3·3·7·529510939·715827883·2147483647·2903110321·658812288653553079
M187 = 196159429230833773869868419475239575503198607639501078527 =
23·89·131071·707983·10326708167438438609988500562789506664915 37
M188 = 392318858461667547739736838950479151006397215279002157055 =
3·5·283·2351·3761·4513·13264529·7484047069·165768537521·140737471578113
M189 = 784637716923335095479473677900958302012794430558004314111 =
7·7·73·127·337·92737·262657·649657·1560007·20761748554425839297075352 7
M190 = 156927543384667019095894735580191660402558886111600862822 3 =
3·11·31·191·2281·174763·524287·420778751·30327152671·3011347479614249131
M191 = 313855086769334038191789471160383320805117772223201725644 7 =
383·7068569257·39940132241·332584516519201·87274497124602996457
M192 = 627710173538668076383578942320766641610235544446403451289 5 =
3·3·5·7·13·17·97·193·241·257·641·673·65537·6700417·22253377·18446744069414584321
M193 = 125542034707733615276715788464153328322047108889280690257 91 =
13821503·616544402332483406165 59·14732265321145317331353282383
M194 = 251084069415467230553431576928306656644094217778561380515 83 =
3·971·1553·11447·31817·1100876018364883721·13842607235828485645766393
M195 = 502168138830934461106863153856613313288188435555712276103 167 =
7·31·79·151·8191·121369·145295143558111·134304196845099262572814573351
M196 = 100433627766186892221372630771322662657637687111424552206335 =
3·5·29·43·113·127·197·19707683773·4363953127297·4432676798593·4981857697937
M197 = 200867255532373784442745261542645325315275374222849104412671 =
7487·268288039979128869297108670418919894904868938457124488 33
M198 = 401734511064747568885490523085290650630550748445698208825343 =
3·3·3·7·19·23·67·73·89·199·683·5347·20857·153649·599479·33057806959·242099935645987
M199 = 803469022129495137770981046170581301261101496891396417650687 =
164504919713·488416409388394117766004909858632430297754360079 9
M200 = 160693804425899027554196209234116260252220299378279283530137 5 =
3·5·5·5·11·17·31·41·101·251·401·601·1801·4051·8101·61681·268501·340801·2787601·3173389601

Weitere (zum Teil komplizierte) Mersenne-Zerlegungen:

$2^{257}-1$ = 231584178474632390847141970017375815706539969331281128078915168015826259279871 =
535006138814359·1155685395246619182673033·37455059850181093658177663009631318139 3 78 St.
yafu: 0,9s pari: 5s ct2: 13s

$2^{331}-1$ = 437450144956602384874500445423524273070633886178642487285154121281990599839875184644702635404610764 7 =
16937389168607· 865118802936559·
29854262498019746361376721533356942800568646883582125372179668262555191 9 100 Stellen brent: 13s

$2^{757}-1$ = (228 Stellen)
75806547475620553474071264085083132580902637554526201715774025294240769174139496402874922306086253806176158725445853183895096681841543671457240589601620172812717528126018061794446547149980392813733544882505686950727189787783987 1 =
9815263· 561595591·
57221370220020678242482279750958577491513128278093884069623462531821289169645 93·
24033821640983508088736273403005965446689002356344332130565066643193813901119771090424269412054543072714914742665677774247325292327559

$2^{1061}-1$ = (320 Stellen)
24707306311927565716857342128774085333197833223161879682238935306082805123046306993647507776054336486228891340858985829027076261887914242781617846672453431386903982455635542158748401823985988322905245077938567513252198179128990807936780194781391547404884040101606295111368825026273254703636026307207764436438929167613951 = P143· P177 =
46817226351072265620777670675006972301618979214252832875068976303839400413682313921168154465151768472420980044715745858522803980473207943564433·
52773964281123391755883821607353460931252289625470797201058317576046705489649287270278654976405264349351138227322605263197977553393635146203746433188046718771717925670714830324 7

Einige ausgesuchte Zahlen und ihre Faktorisierung :

digits	Zahl n =	Zeit / s
10	8616460799 = 89681 · 96079 („**JEVON**s" Zahl)	fmt: 0,04
10	4294967297 = 641 · 6700417 (**Fermat F5 = 2^32+1**) Euler; 1732	Prb-Div: 0,04
11	17543877193 = 52579 · 333667	Prb-Div: 0,05
13	4156338464051 = 2038717 · 2038703	fmt: 0,04
14	18128486155487 = 4257749 · 4257763	fmt: 0,04
15	239812014798221 = 15485863 · 15485867	fmt: 0,03
16	1001001000000007 = 64513 · 15516268039	Prb-Div: 0,05
17	68442389367182561 = 15485863 · 4419669047	Prb-Div: 0,12
18	914561491635920053 = 323769703 · 2824728451	Leh: 0,7
18	965521343020615207 = 982609429 · 982609483	Fmt: 0,04
19	8115469396070122309 = 3013189513 · 2693315293 Fmt: 0,4s	Leh: 1,2
19	12484364901064956197 = 2824728451 · 4419669047	Fmt: 6,8 Leh: 3,2
20	18446744073709551617 = 274177 · 67280421310721 (**Fermat F6 = 2^64+1**) zerlegt von Clausen 1855; unveröffentlicht sowie Landry/Lasseur 1880	brent: 0,04 Prb-Div: 0,04
21	4157584655338486429 67 = 11110693267 · 37419669101	brent:0,04
24	662835905978993515936337 = 724170440549 · 915303730813	brent: 0,07
26	33333332222222222218888889 = 29999999 · 1111111111111111111	Prb-Div: 0,6
32	79798272259984334113870248395353 = 1303 · 6763 · 10627 · 16927 · 29947 · 157543 · 10670053	Prb-Div: 0,04
34	12408190028675983612802100274871 89 = 538119463428139 · 2305843009213693951	brent: 14
37	2310000000000000000000000000000000000 = $2^{34} \cdot 3 \cdot 5^{34} \cdot 7 \cdot 11$	Prb-Div: 0,03
39	340282366920938463463374607431768211457 = *zerlegt von Morrison & Brillhart; 1970* 59649589127497217 · 5704689200685129054721 (**Fermat F7 = 2^128+1**)	brent: 34 pari: 0,02
42	$10^{41}+1$ = 100000000000000000000000000000000000000001 = 11 · 2670502781396266997 · 3404193829806058997303	pari: 0,3 brent: 335
42	100000000000000000507000000000000004563 = 10000000000000000117 · 100000000000000000039	Leh: 12
46	14272476927059598804393159475009619897194905 61 = 2305843009213693951 · 6189700196426901374495621 11 = **M61** · **M89**	brent: 276
49	85779122932654454031623614621629972200431028761 99 = 12764787846358441471 · 671998030559713968361666935769	pari: 0,3 yafu: 0,4
55	675062234896414305195630546932696211776378888978198538 7 = 7 · 97 · 997 · 9973 · 99991 · 999983 · 9999991 · 99999989 · 999999937 · 9999999967 dies ist das Produkt der jeweils größten ein-, zwei-, drei- bis zehnstelligen Primzahlen	brent: 0,04
59	$(5^{91}-1)/(5^{7}-1)$ = 516994500375247099957509888670301763341203336715759278125 01 = 305175781 · 968064779056858908635555 9 · 1749973366315297653345251 9	yafu: 0,6 ct2: 0 (0) pari: 0,2 Til: 1,6
60	100433627766186892221372630609062766858404681029709092356097 = 6189700196426901374495621 11 · 16225927682921336339157801028812 7 = **M89** · **M107**	yafu: 1,9 ct2: 0 Til: 0,5 brent:
61	$(2^{214}+1)/4285$ = 61442410541748650348843656758267463429927126838126669343238 61 = 843589 · 8174912477117 · 23528569104401 · 37866809061660057264219253397	brent: 6 Til: 17
68	19319597769065583697597909403141892104992276797595838342261048259737 = 25424590664090308146038848774534 73 · 75987841945288753799392097264437 69	Yafu: 9,9 ct2: 2 (11) pari: 13 Til: 1,5
68	24284712165828060817808704394685584572191120513988451223045457718339 = 29996224275833 ^{2} · 29996224275851 ^{3}	
71	27606985387162255149739023449107931684587161426206011699548030008033 29 = 16225927682921336339157801028812 7 · 17014118346046923173168730371588410572 7 = **M107** · **M127**	yafu: 15,5 ct2: 2 (19) pari: 22 Til: 2,3
75	513083011646316351481885794652483810265929673418478017639835191953430902707 =	yafu: 39

	136986301369863013698630136986301369863013699 · 3745505985018109365817766300963131813931	ct2: 9 (53) pari: 70 Til: 4,9
78	11579208923731619542357098500868790785326998466564056403945758400791312963993 7 = 1238926361552897 · 93461639715357977769163558199606896584051237541638188580280321 (**Fermat F8 = 2^256+1**) zerlegt von Brent & Pollard; 1980 [brent: 56s]	ct2: 10 (45) yafu: 0,7 pari: 1 Til: 5,7
80	25389739913858345524208216151645759882986445317021182277812631082013053557679073 = 57841295759118288267473253993921326751 37 · 43895524089907382652596083010742568073 29	yafu: 67 ct2: 16(96) pari: 202 Til: 9,8
83	18160190347537855674572437704347670349236701129933651524793994702762718415306289 571 = 352335940104882765046233099089267620035 13 · 515422591919858105130783469902677253473467	
84	23986136625956052485865148735412958823329151363927624346327130843836030789585592 1843 = 489756435648946347624324859824637632984391 · 48975643564894634762432485982463763298437 3	yafu: 0,01 ct2: 33(264) pari: 697 Til: 20 **Progr.„Fermat" löst in 0,03s !!**
85	(11^93+1)/5823582370884 = 12143097918088867233227584561865518009470962182715685846053337560098991375703209766 23 = 237843323473654847623 · 365852473845513195122 3 · 139550866104193032581962716205911186751428 7	yafu: 3,9 ct2: 36 (233) pari: 11 Til: 3,2
87	(5^128+1)/514 = 57173849748165734823382127296801832578728869492805813302954849527160372541572333309900 9 = 23653200983830003298459393 · 24171717725330873572798545219226642215966994254472458802413313	ct2: 68 (399) Til: 39 yafu: 4,7 pari: 80
88	38353230902979262626847647698929219318455512236590939056458280995140151560618248 17478743 = 7432339208719 · 341117531003194129 · 15127682224137352558644030052641058393243747785206318539 93	Yafu: 0,9 ct2: 84 (41) pari: 7 Til: 54
94	17375855758549154624366762941835019305510457496880844836981879745085135987501018 73166735739991 = 23096923021977474330660193223430446887477 43 · 75230175647273284335652420066607907427136274861453 7	yafu/s: 10 pari: 10852 ct2: 328(1826) Til: 169
100	43442698883654206465611893379827125408623206550910149411977322744011293292242275 19682504576978654093 = 58219095811886820515178767227081790299538366398541 · 74619329410444640929930650594192092128852582596673	yafu/s: 4567 ct2: 1548 msi: 8201 pari: - Til:
100	15226050279225333605356183781326374297180681149613806886579084945801229632589528 97654000350692006139 = 37975227936943673922808872755445627854565536638199 · 40094690950920881030683735292761468389214899724061 LOG IN Heft Nr. 172/173 (2011/2012)	yafu: 3893
109	(5^160+1)/1282 = 53371900607145248472073115100684817548883806654203780552126052885 57426303375236909669637698215227603168457793 = 75068993 · 241931001601 · 46957667265666758402894952584920394200961 · 62582663240692632675871452234418855417095109446 41	yafu: 708 ct2: 1885 pari: 4410 Til: 807
121	73281095113106734398239989296282702447648950464623884587479737832729774008066025 61983902737712247132163867744658163132181 = 2756163353 · 598990818061 · 4527716228491 · 248158049830971629 · 33637310674071348724927955857253537 · 11744593722752035313978951707661039 9	yafu: 18 pari: 35 ct2: 2d (476) Til:
134	(10^142+1)/440729761 = 22689640874966916518260721676111180519983083239073569166117 64731721849843491735517266327744088967933345440676968488179766920709491184 1 = 380623849488714809 · 77169265188335087786895085049 41 · 93611382287513950329431625811490669 · 82519882659061966708762483486719446639288430446081 (1991 faktorisiert)	yafu/s: > 1d msi: > 1d ct2: 24 Tage ! pari: 1789 Til:
137	(2^484+1)/1254743089 = 39807333662911990505576361597868630214848364295425530264663 21613189291518872533907371447387108570999155129110094863887018959911630851195 3 = 33186913 · 1251287137 · 2931542417 · 38608979869428210686559330362638245355335498797441 · 84694409197705740057696939084347325062258739942360856026657 29	yafu:Absturz nach 30s ct2: 11326 msi: 51156 pari: Abbruch Til: 7575
155	13407807929942597099574024998205846127479365820592393377723561443721764030073546 97680187429816690342769003185818648605085375388281194656994643364900608409 7 = 2424833 · 74556028256478842083373957362004549187833663426 57 · 74164006262753080152478714190193747405994078109751902390582131614441575950470500 8092818711693940737 (**Fermat F9 = 2^512+1**) zerlegt von Lenstra & Manasse; 1990	yafu: > 2d ct2: 3968d pari: Til:
162	(12^151-1)/11 = 82219620528659701952660120743076100427390924357073396551677033937335320743050235802427303275633200540806689460669679221954509396712733084562446 2896060630268212317 = 16537237851564688924261407041648853990657743 ·	yafu:Absturz ct2:

	4971786780032337881876339900596001648747659834953921156974700575915322824191116 7 043200927016884285731030248831349126419 (1993 faktorisiert)	pari: Abbruch nach 20 h
170	50^{100}-1 = 7888609052210118054117285652827862296732064351090230047702789306640624 9999999999999999999999999999999999999999999999999999999999999999999999999 9999999999999999999 = 3 ·7 ·7 ·11 ·17 ·41 ·61 ·101 ·151 ·251 ·62801 ·535151 ·557041 ·5122541 ·6377551 ·7622561 ·109461 01 · 389204401 ·10226070591601 ·890341129892310 1 ·10604434965481801 ·3032278293370078 01 ·371550266777255565 1 ·13874227772299098146101	max: 25s yafu: 0,8s ct2: ca. 4h brent: 686s Schö: 2s
202	6592309255872567236671567108937399262061067258329011901925136502092615689205076 0 6065172489394540316660737278499039707243803129856565681278595584288485116218855 6 539495554272669866793569293859644799976733 = 8119303699131205202113628702455086873261724383429839878221301725116680814438295 4 024225441452897752819 ·811930369913120520211362870245508687326172438342983987822 1 3017251166808144382954024225441452897753007	Fmt: 0,03 Leh: 1
211	1451227665928429038078135931392086641805560994157364861845488884120406459417175 2 0737675249476056266570789846568758842739759419609137155408009079513754326016948 9 098207940366177919426111059426911414577902662170527 = 47·523·599·2417·1523·8191·32497·11491·4639· 196717· 48397· 100673· 178481· 993683· 489553· 1126847· 2299159· 9316273· 9341359· 17094767· 7504421· 14718679249· 13444476836590589479· 51441563151591093599· 26024244971250991615 9· 29592773689035264646070825945299759722 1 Anmerkung zu * : Pari sowie ct2 und Til benötigen die von kleinen Faktoren bereinigte 98-stellige Zahl 53262540262425205280262026385973461969480438549 544936590070499414516458337155618640383132016518019	yafu: 2,8 ct2: 908 * pari: 16 * Til: 404 *
284	(2^{953}+1)/5721 = 1330803455935369565028155915142019029517925578132511734026490459 6 5698587041798119079728400108727853784649003072990526516663651048019400755530310 3 0545786157112408338932163947831824076941708799882495411086183603143672551780072 0 411572301421894329402716046524575072980542451628711517762 33 = 425796183929· 1624700279478894385598779655842584377· 380230673854944132443213909127182812 1 ·1280648868301666714448025761291158720602 7 · 338849583746672139436839320467218152281583036860499304808492584055528117 7· 1165882340667125990314837655838327081813101225814639260043952099413134433416292 4 536139 (2002 faktorisiert)	yafu: einige Tage ct2: Absturz msi: Abbruch pari: / Til: Abbruch
309	1797693134862315907729305190789024733617976978942306572734300811577326758055009 6 3132708477322407536021120113879871393357658789768814416622492847430639474124377 7 6789342486548527630221960124609411945308295208500576883815068234246288147391311 0 540827237163350510684586298239947245938479716304835356329624224137217 = 45592577· 6487031809· 4659775785220018543264560743076778192897· 1304398744054881897274847687965099039466085308416118921868952957768324162514718 6 3574140227977573104895898783928842923844831149032913798729088601617946094119449 0 1059590671013053190617101835449160961919391248853811608071229967232280621782075 3 127014424577 (**Fermat F10 = 2^1024+1**) zerlegt von Brillhart 1962 ; Brent 1995	yafu: 2601 Til: Abbruch pari: / msi, c2t: Eingabe > 10^274
313	2^{1039}−1 = 58906808643168367664473872491774762471193869645981501775357568993765843 2 0794655559932591384900650140340063891615625817543763223144510803885845624607194288 1 0761069833174599222153387113189363201210623862217392146903328852155899782370013718 4 80620182690736866953411252382072659135491210334387684495620912657652829388 7 = 5080711· 5585366661993629126074920465831594496864652701848863764801005234631985 3 288374753· 2075818194644238276457048137035946951629397080073952098812083870379 27 2909032467938234314388414483488253405334476911222302815832769652537609141018910 5 24199389933410971162435896206597216748116174900480365973557340925320542552368 (**Mersenne M1039**) zerlegt von Thorsten Kleinjung; 2007	yafu/s: Ausstieg pari:
335	960^{119}−1 = 577674189759733695792431849194721730257718954139100278378828062037 24 8311742658685209611920240447476391973748107474391563802565902798573585394810432 1 0653517614207243140020936698427063888415532640577479326636213888470839711331739 5 7981634559999999999999999999999999999999999999999999999999999999999999999 99999999999999999999999999999999999999999999999 = 7 ·7 ·71 ·137 ·239 ·463 ·911 ·23291· 18306961· 3737870641· 62564321333· 1152147740399· 6720387718367512278456965653424503150621415515594735646424346745 41 · 2093854829168447724592706233803785431818384929051619909027858304395414102119083 4 8988366141813918264438047589537949445601366504530497103435887842062558424042444 2 5748326295405066952886207632798554957218345015204890988777599467406393 47	yafu/s: Ausstieg msi: Ausstieg ct2: Ausstieg Til: Ausstieg pari:
617	3231700607131100730071487668866995196044410266971548403213034542752465513886789 0 8931972014115229134636887179609218980194941195591504909210950881523864482831206 3 0877367300996091750197750389652106796057638384067568276792218642619756161838094 3 3847617047058164585203630504288757589154106580860755239912393038552191433338966 8 3424206849747865645694948561760353263220580778056593310261927084603141502585928 6 4177116725943603718461857357598351152301645904403697613233287231227125684710820 2 0972515710172693132346967854258065669793504599726835299863821552516638943733554 3 602135433229604645318478604952148193555853611059596230657 =	yafu: 15 pari: 241 Til: Abbruch

	319489· 974849· 167988556341760475137· 3560841906445833920513· 1734624471791475554302589708643097783774218447236640846493470190613635791928791088575910383304088371779838108684515464219407129783061341898642808260145427587085892438736855639731189488693991585455066111474202161325570172605641393943669457932209686651089596854827053880726458285541519364019124649311825460928798157330577955733585049822792800909428725675915189121186227517143192297881009792510360354969172799126635273587832366471931547770914277453770382945849189175903251109393813224860442985739716507110592444621775425407069130470346646436034913824417233065988341774177 (**Fermat F11 = 2^2048+1**) zerlegt von Brent & Morain; 1988	

Semiprimzahlen

Eine **Semiprimzahl** ist eine natürliche Zahl, die zerlegbar ist in ein Produkt aus **genau 2** Primzahlen .
Es handelt sich also hier nicht um eine Primzahl !
Die ersten Semiprimzahlen sind 4 (=2·2) 6 (=2·3) 9 (=3·3) 10 (=2·5) 14 (=2·7) 15 (=3·5) 21 (=3·7)

Beispiel 1: 80313965845625220873194079672 1
besteht aus 30 Ziffern (100 Bits) und lässt sich zerlegen in
878529705721751 · 914186114852471
Yafu: 0,17s brent(Ac): 8s Lehman(Ac): 0,3 s

Beispiel 2: 713623846352979940529142984724747568191373311
besteht aus 45 Ziffern (149 Bits) und lässt sich zerlegen in
86656268566282183151 · 823510933669084672398616 1
Yafu: 0,26s pari: 0,1s

Beispiel 3: 38!+1 = 523022617466601111760007224100074291200000001 =
45 Ziffern (149 Bits)
37280713718589679646221 · 14029308060317546154181
Yafu: 0,3 s pari: 0,1s

Beispiel 4: 10^{48} + 19 = 100000000000000000000000000000000000000000000019 =
49 Ziffern (160 Bits)
17507530776122167975943559 13 · 571182774308676717563
Yafu: 0,4s pari: 0,2s

Beispiel 5: 85397342226735670654637567334028930584606539118838378 3 =
54 Ziffern (180 Bits)
27182818284590452353603 53 · 31415926535897932384626433831 1
Yafu: 1s Til/P: 0,5s pari: 0,6s

Beispiel 6: 71641520761751435455133616475667090434063332228247871795429
besteht aus 59 Ziffern (196 Bits) und lässt sich zerlegen in
35744050410138836561078538901 7 · 2004292181208155542697436354 37
Yafu: 2s Til/P: 0,5s pari: 2,5s

Beispiel 7: 10^{63} + 19 = 100000000000000000000000000000000000000000000000000000000000000019
= 64 Ziffern (210 Bits)
44741590990368441481914582608543 · 22350568628980377780095228766733
Yafu: 3,5s Til/P: 0,7s

Beispiel 8: 729346944528564617209248390517758983860666588441034039195491780030381328027527 9
besteht aus 79 Ziffern (262 Bits) und lässt sich zerlegen in
84818438291948899360848100931373480897 7 · 85989197539586788824000429721336460377 27
Yafu: 65s Til/P: 11s pari: 216s

Beispiel 9: 16368054432676235348632643877118481207371456933092253539382430638081302047541099874017838 57 =
91 Ziffern (300 Bits)
13485329506402520485674964872111548148784559687 71 ·
12137674815365144903021465040591855759822 67
Yafu: 7s Til/P: 89s

Beispiel 10:
11288798737163099824081460333619591342348211143669600740142907237723834164788215269828
1999652360869 =
99 Ziffern (326 Bits)
36190234934785044449782293780001398745689734619 37 ·
31192941293433332564432124322469839822238973411637
Yafu/s: 3510s Til/P: 513s

Beispiel 11: $(11^{104}+1) / (2 \cdot 17 \cdot 6304673) =$ 941234360735926294697117213629451435752898137898308254134753221194264012130159069863408961146891168 1 =

100 Ziffern (333 Bits) - wurde 1988 faktorisiert mit MPQS

867592223134283908122180770958507080489 77 ·

108488104853637470612961399842972948409834611525790577216753

pari: 20635s ct2: 798s msi: 10s yafu: 2671s Til/P: 416s

Beispiel 12: 288103982745789597188162705313753073463879082516612749606667432024157144649476238662044295382073545 3 =

100 Ziffern (331 Bits)

618162834186865969389336374155487198277265679 ·

466064872898356637396439537520952929159659540064606830 7

yafu/s: 4279s Til/P: 632s

Beispiel 13: 183057933638066122894639995986161133790517848510554938669449171162804218060563619208165224369374109411838369973616878561 7 =

121 Ziffern (400 Bits)

785506617513464525087105385677215644061830019071786760495463 ·

233044419431550225562286848781148674808128493437968665268915 9

yafu/s: Ausstieg Til/P: pari:

Beispiel 14: $(6^{353}-1) / 5$ = 973691505184416442565958983076531038101774699445446034442467673403970145084942466298465294694187891794816051886144204066226423206167081784681898063663685509304513573706979052346135130666317823161124260153050164931265319361687960957823878998047485678787428763591656991956664 3 =

274 Ziffern (911 Bits)

135095261330112651830775049635590807381121031111382732318390846759744072165636542920143351738198057636666351316191686483 ·

720744381111301937643935864029025391613890867099707817049849566271785734074845094811610876273732867041786794660514517682420730722427836886613902736846235 21

yafu/s: Til/P:

RSA – Zahlen

RSA-Zahlen sind Semiprimzahlen (s. oben !), welche in der sogenannten Factoring Challenge of RSA Security (ein mit Preisgeldern ausgelobter Wettbewerb) gelistet waren ;
Bezeichnungen: RSA-100 etc. bis RSA-500 .

Diese Zahlen sind schwer zu faktorisieren, wenn sie genügend groß sind (etwa 100 Ziffern und mehr !) .
Daher werden sie in der **Kryptographie** verwendet.
Benannt wurden sie nach den Wissenschaftlern **R**IVEST, **S**HAMIR und **A**DLEMAN.

Berühmtes Beispiel für eine RSA-Zahl aus „Spektrum der Wissenschaft“:

Die **129-stellige** Zahl „**RSA-129**“ =
```
114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
```
(426 Bits)

ist Produkt zweier Primzahlen. Wie lauten diese Faktoren?
Diese Frage stellte **Martin Gardner** (1914 - 2010) den Lesern des Scientific American im August 1977 in seiner Kolumne "Mathematical Recreations".
Im Gegensatz zu den Rätseln, die Gardner sonst aufzugeben pflegte, musste dieses ungewöhnlich lange auf eine Lösung warten. Erst mehr als 16 Jahre später, **im April 1994**, präsentierten Paul Leyland von der Universität Oxford, Michael Graff von der Universität von Iowa in Iowa City und Derek Atkins vom Massachusetts Institute of Technology in Cambridge die 64- bzw. 65-stelligen Primfaktoren

```
349052951084765094914784961990389813341776463849338784399082057 7    sowie
327691329932667095499619881908344614131776429679929425397982885337
```

Beispiel 2: RSA-100 =
```
152260502792253336053561837813263742971806811496138068865790849458012296325895289765400035069200613 9
```
(100 Ziffern; 330 Bits) ; wurde 1991 faktorisiert mit MPQS
```
37975227936943673922808872755445627854565536638199·
40094690950920881030683735292761468389214899724061
```
```
yafu: 20s     ct2: 5760s      Til/P: 3521s       pari: ?s
```

Beispiel 3: RSA-120 =
```
227010481295437363334259960947493668895875336466084780038173258247009162675779735389791151574049166747880487470296548479 =
```
(120 Ziffern; 397 Bits) ; wurde 1993 faktorisiert
```
33274145556934980157511463037491414880636424032401714634068 83·
69334266711083018119732540189970064136196586312733668067301 3
```

Beispiel 4: RSA-140 =
```
212902463182587575474978820162715174978067039632772162782333832153819499840564959113665738530219183167831073879953172308895692308734419364 71 =
```
(140 Ziffern; 463 Bits) ; wurde 1999 faktorisiert
```
33987174230284385545301236276138758356339864959695974234909293027714 79·
62642001874012850961516549482644422193020371786235090191116606539460 49
```

Beispiel 5: RSA-170 =
```
260626236841398449215298792666744321970859253804864064161647851918599996285420693614502839319145146186835121981648059198820530572229741164780650958098323773365107115457 59 =
```
(170 Ziffern; 563 Bits) ; wurde 2009 faktorisiert
```
35864207304285014867998045872685204232914596810599781611402318606339484508580405939 63·
72670290641070190788637977639239462641361378038569966703137089360022815822495874944 93
```

Weitere Beispiele für RSA-Zahlen

RSA 200

```
RSA-200 = 27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983 =
```
(200 Ziffern; 663 Bits)
```
35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883490·
79258699544783330333470858414800596877379758573642199607343303414557678728181521353814093047401854 67
```
zerlegt 05-2005 von Gruppe Prof. Jens Franke

RSA 260

```
RSA-260 = 22112825529529666435281085255026230927612089502470015394413748319128822941402001986512729726569746599085900330031400051170742204560859276357953757185954298838958709229238491006703034124620545784566413664540684214361293017694020846391065875914794251435144458199
```
Bis heute noch **nicht** zerlegt !

RSA 270

```
RSA-270 = 23310853034440754452763765691068052414561981248030544904294861196849591824513578286788836931857711641821391926857265831491306067262691135402760979316634162669394659619642774427388660187689631346870405906674690312391074827760654864915192081269930976658751473545659499320 7
```
Bis heute noch **nicht** zerlegt !

RSA 400

```
RSA-400 = 20140968789452075117267004857834425479153217820727043561030391290099667933961419850865094551022604032086955587930913903404388675137661234189428453016032619119305676856486261532125663001026834647174783659713139894314068546405163175194031492943087373023216848409563951832221174684435785098479471199953736453607109795994713287610750434646825511120586422993705980787028106033008907158745005847581468494 81
```
Bis heute noch **nicht** zerlegt !

RSA 576

Die Primfaktorzerlegung dieser 174-stelligen Zahl wurde im Dezember 2003 von Jens Franke und Thorsten Kleinjung vom Mathematischen Institut in Bonn und dem Institut für Experimentelle Mathematik in Essen gefunden. Das Preisgeld lag bei 10.000 US$.

```
RSA-576 = 188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059 =
3980750864240649373971255005503864911990643623425267084063851895759463889572617685833317 ·
4727721461074353025362230719730482246329146953020971164598521711305207112563635903975 27
```

Anmerkung zur (anscheinend verwirrenden) Bezeichnung der RSA-Zahlen:

Die ersten erzeugten RSA-Nummern von RSA-100 bis RSA-500 wurden entsprechend ihrer Anzahl von Dezimalstellen gekennzeichnet.
Später, beginnend mit RSA-576, werden stattdessen Binärziffern gezählt.
Eine Ausnahme bildet RSA-617, das vor der Änderung des Nummerierungsschemas erstellt wurde !

RSA 640

Die Faktoren dieser 193-stelligen Zahl wurden im November 2005 von F. Bahr, M. Boehm, J. Franke, T. Kleinjung gefunden, die zuvor schon RSA 200 faktorisiert hatten. Das Preisgeld lag bei 20.000 US$.

```
RSA-640 =
3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609
```

wird zerlegt in

```
1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579 ·
1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571
```

RSA 768

Die Faktorisierung dieser 232-stelligen Zahl wurde am 12. Dezember 2009 von Thorsten Kleinjung et al. vollendet.[1] Der RSA Factoring Challenge war zu dieser Zeit schon beendet, sodass kein Preisgeld ausgezahlt wurde.

```
RSA-768 =
123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346391602221240479274737794080665351419597459856902143413 =

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489 ·
36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917
```