Nikolaus Castell-Castell
Tom Tietken

Prag, im Juli 2020

Das Faktorisieren grosser Zahlen mittels des neuen CASTELL-FACT-ALGORITHMUS, 12. Teil.

Als Teilaspekt hier die Einfuehrung des neuen TIETKEN-CASTELL-PRIM-ALGORITHMUS zur indirekten, eindeutigen und korrekten Identifizierung und Herstellung von Primzahlen (prime numbers) unbegrenzter Groesse.

Zielsetzung

Werden fuer die Faktorisierung grosser Zahlen grosse Zahlen vorgelegt, die verlaesslich aus der Multiplikation von zwei Primzahlen entstanden sind, taucht die folgende Frage nicht auf.
Ist es aber fraglich, ob die vorliegende "grosse Zahl" ein Produkt aus zwei Primfaktoren ist oder selbst eine Primzahl (die nicht faktorisiert werden kann) oder vielleicht auch nur ein Produkt, das mit den Ziffern 1, 3, 7 oder 9 endet, muss es eine zuverlaessige Moeglichkeit der Klaerung geben, festzustellen, was die vorliegende grosse Zahl darstellt.

Wenn man einen Blick auf die vielen bisherigen, nicht verlaesslich und eindeutig funktionierenden, Loesungsmoeglichkeiten wirft, weiss man, dass hier ein neuer Ansatz ohne unsichere Mehrfach-Versuche und ohne Fehlerquoten (Fermat, Miller-Rabin, chinesische Restsaetze, Mersenne-Vermutung u.v.a.) und ohne Wahrscheinlichkeitsrechnung, Annaeherungen und Wiederholungen usw. benoetigt wird, der mehr als nur ein "most likely prime" liefert.
Denn selbst die RSA (Ron Rivest, Shamir, Adleman) verwendet nur "Zufallszahlen", die keine 100%-igen Primzahlen liefern, sondern sog. "Wahrscheinlich-Primzahlen".

Die neue Idee des TIETKEN-CASTELL-PRIM-ALGORITHMUS erspart dem Anwender die o.g. Unsicherheiten und Ungenauigkeiten. Sie liefert eindeutig jederzeit und in allen Groessenordnungen "100% Primzahlen".

Sie vermeidet auch den Nachteil, der bei dem RSA-Multiplizieren von zwei identischen Primzahlen, naheliegend ist, naemlich, dass durch die grossen Spruenge nach Vorne (s. grosse

Primzahlen mit sich selbst multiplizieren) andere, kleinere Primzahlen, die unterhalb dieses Sprunges liegen, uebersehen und uebergangen werden, kurz gesagt, dass in der Vorstellung, welche Primzahlen es denn sonst noch gibt, Unordnung entsteht. Bestuende totale Klarheit und Transparenz, muesste kein Verschluesseler aus Sicherheitsgruenden, "wahrscheinliche" Primzahlen mit sich selbst multiplizieren.

Persoenliche Vorbemerkung zum TIETKEN-CASTELL-PRIM-ALGORITHMUS

Der hier vorgestellte, neue Tietken-Castell-Prim-Algorithmus kann nicht nur Primzahlen auf indirekte Art identifizieren, sondern diese auf indirekte Art auch selbst herstellen.
Die Loesung, die das o.g. neue Prozedere vorschlaegt, ist einfach und naheliegend.

Eine Primzahl herzustellen, deren Laenge ein Dutzend Aktenordner fuellt, mag eine beeindruckende Vorfuehrung der quantitativen Moeglichkeiten von Rechen-Maschinen sein, hat aber, abgesehen von dem ersten Nachdenken ueber den Algorithmus fuer die noch relativ kleinen Primzahlen am Anfang, nichts mit qualitativ anwachsendem menschlichen Denken zu tun (vgl. Gimps und 400 Jahre alte Mersenne-Zahlen u.a.). Es ist eine (derzeit noch nutzlose) Vorfuehrung mit hohen Stromkosten und minimaler menschlicher Eigenleistung.

Verbale Erklaerung des TIETKEN-CASTELL-PRIM-ALGORITHMUS

Die Grundueberlegung fuer den vorliegenden Tietken-Castell-Prim-Algorithmus ist, die noch bestehende Unmoeglichkeit, Primzahlen rasch zu erkennen und herzustellen, auf indirekte Weise zu erreichen.

a)
Sind Primzahlen nicht einfach und korrekt herstellbar, kann fuer ihre Herstellung auf Pendants zurueck gegriffen werden, die im Differenzverfahren entstehen und im Idealfall (wie hier) exakt berechenbar sind. Das sind hier die wohl-geordneten auf der einen Seite konstant bleibenden Zaehlfaktoren und auf der anderen Seite die in 2-Schritten kardinal anwachsenden gezaehlten Faktoren der ebenfalls wohlgeordnet und nachvollziehbar anwachsenden nicht-Primzahlen bzw. der Produkte in der Naehe der gesuchten Primzahlen.

Die Primzahlen sind dabei die "Reste". Es sind die Zahlen, fuer die es keine Faktoren gibt!

b)
Wenn auf diese indirekte Weise Primzahlen "hergestellt" werden koennen, dann auf diese Weise, dass sich diese Primzahlen von ihrer Position her identifizierbaren lassen.
Wegen der Einfachheit und wegen des Gleichbleibens aller Schritte und Vorgehensweisen gibt es eine sich in ihren Zahlenwerten aufbauende Reihenfolge von Primzahlen, die keine Fehler oder Luecken aufweisen, d.h. die jede Primzahl erfasst und erkennbar macht.

Der Tietken-Castell-Algorithmus kann, einmal in Bewegung gesetzt, "maschinell", also ohne weiteres menschliches Zutun und ohne weitere eigene Gedankenleistung, ein Register aufbauen, das (ohne neuen Input) stetig groesser wird und auf das, da es nach Zahlenwerten geordnet ist, jederzeit Zugriff genommen werden kann!

Zahlenbeispiele des TIETKEN-CASTELL-PRIM-ALGORITHMUS

Der Tietken-Castell-Prim-Algorithmus baut sich pro Zehnerreihe nur mit den Endziffern 1, 3, (5), 7. 9 auf.
Die 5 wird hier in Klammern geschrieben, da sie eine Ausnahme darstellt. Sie kann (ausser als Einerziffer) auch mit hinzukommenden Dezimalziffern niemals eine Primzahl werden, da Zahlen mit der Endziffer 5 immer durch 5 teilbar sind. Allerdings wird sie in diesem Tietken-Castell-System mitgezaehlt, um eine gleichmaessige Hochzaehlung beizubehalten und bei einer Endzahl "5" nicht jedes mal einen Doppelschritt einlegen zu muessen, bei dem die "5" uebersprungen wird.

Wie sich zahlenwertmaessig, d.h. hier sukzessive und in gleich bleibender Ordnung, das "Tietken-Castell-Register" (das ist der sich zukzessiv aufbauende Zahlenbestand) vergroessert, zeigt die folgende Graphik, die nach unserer Praemisse eines gleichartig bleibenden Dezimalsystems) unbegrenzt weiter fortgesetzt werden kann!

a)
In jeder der unbegrenzt vielen Zeilen werden nur Zahlen mit den Endziffern 1, 3, 5, 7 oder 9 erfasst. Denn jede Primzahl muss 1, 3, 7 oder 9 (die Ausnahme 5 entfaellt) als Endziffer aufweisen.

Allerdings ist nicht jede Zahl mit dieser Endziffer eine Primzahl. Um also saemtliche Primzahlen lueckenlos zu erfassen, muessen saemtliche Zahlen, die eine der vier Prim-Endziffern aufweisen, mit in das Register aufgenommen werden. Unter ihnen befinden sich auch die Primzahlen. Zu identifizieren sind sie damit, dass es fuer sie keine Faktoren gibt.

b)

Die Zeilen des Tietken-Castell-Registers sehen immer gleich aus. Alle Zeilen weisen die Endziffern 1, 3, 5, 7 und 9 auf. Und jede weitere hinzukommende Zeile erhaellt eine Zehnerdezimal-Stelle zusaetzlich:

1 3 5 7 9
11 13 15 17 19
21 23 25 27 29
31 33 35 37 39
41 43 45 47 49
51 53 55 57 59
61 63 65 67 69
71 73 75 77 79
usw.
oder:
1001 1003 1005 1007 1009
1011 1013 1015 1017 1019
1021 1023 1025 1027 1029
usw.

oder:
2381 2383 2385 2387 2389
2391 2393 2395 2397 2399
2401 2403 2405 2407 2409
2411 2413 2415 2417 2419
usw.

c)
Es wird hier also behauptet, dass es keine Begrenzung der Zahlen nach oben hin gibt! Allerdings wird hier keine ca. 2-Millionen-stellige Primzahl gesucht, sondern vorerst "nur" 1.000- bis 2.000-stellige "grosse Zahlen", die durch Multiplikation aus zwei Primzahlen entstanden sind.

Nach hiesiger Einschaetzung kann diese Aufgabe (selbst unter der Praemisse, dass die Primzahlen mit anwachsenden Zahlen immer seltener werden) leichter und schneller bewerkstelligt werden, als in einem unuebersichtlichen Meer von Moeglichkeiten, Primzahlen nach dem Zufallsprinzip zu finden und anschliessend das Problem zu haben, diese Zahl zuverlaessig als Primzahl zu identifizieren.

Der hierfuer noetige Tietken-Castell-Prim-Algorithmus muss dafuer lueckenlos hochzaehlen, durchgaengig addieren, die ununterbrochene Verbindung mit den vorangegangenen Faktoren halten und auch Multiplikationen zwischen zwei Primzahlen herstellen und sich deren Ergebnisse als "grosse Zahlen" merken, um sie spaeter mit ihren mitgelieferten Faktoren abrufen zu koennen!

d)
Um nur Zahlen mit den Endziffern 1, 3, 7 oder 9 im Register zu erhalten, werden saemtliche Zahlen mit den Endziffern 0, 2, 4, 6 oder 8 aus dem Register ausgeschlossen. Die 5 wird im Register mitgezaehlt, spielt aber keine weitere Rolle.

e)
Jede Zahl des o.g. Registers stellt sich also selbst als konstanten Faktor fuer eine eigene Zahlenreihe von weiteren Zahlen (in Abstaenden von 2 mal die jeweilige Zahl) zur Verfuegung.

Immer, wenn sich wegen fehlender Faktoren, die sie hergestellt haben koennten, eine Zahl als Primzahl herausstellt, wird auch diese mit sich selbst multipliziert und beginnt ab der Stelle des entstandenen Produkts (einer "grossen Zahl" aus zwei Primzahlen) eine neue und unbegrenzte Zahlenreihe im Register.

Primzahlen sind Zahlen, die im Tietken-Castell-Register ohne Faktoren auftreten. Sind aber Faktoren (zwei oder mehr) an der Entstehung der vorliegenden Zahl beteiligt, handelt es sich bei dieser nicht um eine Primzahl.

Da die entsprechenden Faktoren "links" in der Vergangenheit liegen, wird dort schon das Produkt errechnet. Taucht dann die in der Vergangenheit errechnete Zahl auf, ist sie bereits als Produkt, zusammen mit ihren Faktoren, bekannt. So kann auch festgestellt werden, ob es sich bei der vorliegenden Zahl um eine "grosse Zahl" handelt, d.h. um ein Produkt aus zwei Primzahlen.

f)
Im folgenden wird die Wirkungsweise der Zahlen im Tietken-Castell-Prim-Algorithmus veranschaulicht. Zwangslaeufigerweise beginnt der Anfang mit kleinen Zahlen. Das Prinzip der Vorgehensweise und des Nutzens setzt sich aber genau wie am Anfang auch nach oben hin unbegrenzt fort, denn die Gesetzmaessigkeiten des Dezimalsystems bleiben fuer kleine und grosse Zahlen dieselben, und die immer gleiche Vorgehensweise des Tietken-Castell-Prim-Algorithmus aendert sich ebenfalls nicht.

g)
1. Zeile, 1. Zahl: 3

Die 3 wird, wie alle Zahlen des Registers, mit sich selbst multipliziert, ergibt 9 und beginnt ab hier die erste Zahlenreihe, die sich durch saemtliche, immer groesser werdende, Zahlen des Tietken-Castell-Registers hindurchzieht.

Diese 3 bleibt als zaehlende Konstante erhalten und bildet erst mit sich selbst, d.h. mit der 3, und danach mit den ungerade Zahlen 5, 7, 9, 11, 13, (15), 17, 19, 21, 23, (25), 27, 29 31, 33,(35), 37, 39 usw. neue Zahlen, die manchmal normale Produkte sind, aber manchmal auch Produkte aus zwei Primzahlen sind.
3 ist eine Primzahl, da sie im Register keine Faktoren von links hat.
Wird sie multiplziert mit z.B. 11 oder 13, fuer die das Gleiche gilt, stellt das entstehende Produkt 33 oder 39 solche zum Verschluesseln geeignete "grosse Zahlen" dar.

Bei den immer haeufiger werdenden Zahlenreihen, die sich unbegrenzt lang durch das gesamte Register ziehen, kann es bei Zahlen, dort, wo sich Zahlenreihen ueberschneiden, Mehrfachbelegungen geben, was bedeutet, dass die betreffende Zahl mehrere Faktoren hat. Am wichtigsten fuer den Tietken-Castell-Prim-Algorithmus ist es aber in diesem Zusammenhang, festzustellen, ob sie ueberhaupt Faktoren hat. Hat sie naemlich Faktoren, kann eruiert werden, ob diese Faktoren prim waren und sich das Produkt als "grosse Zahl" fuer die Kryptographie eignet. Hat sie keine Faktoren, handelt es sich (wie bereits betont) selbst um eine Primzahl. In diesem Fall kann es auch keine Mehrfachbelegungen geben.

h)
1. Zeile, 2. Zahl: 5

Die 5 ist eine Primzahl, weil, wie bei der 3, keine Faktoren zu ihr hinfuehren.
Ihre Zahlenreihe beginnt ab 5 * 3 = 15, wird aber mit ihren hinzukommenden Dezimalziffern niemals mehr eine Primzahlen sein, da sie stets durch 5 teilbar sein wird.

i)
1. Zeile, 3. Zahl: 7
Die 7 ist eine Primzahl und beginnt mit 7 * 3 (= 21) als 7er-Reihe ihren unlimitierten Marsch durch das Tietken-Castell-Register.

i)
1. Zeile, 4. Zahl: 9

Die 9 ist eine Zwischenstufe der 3er-Reihe und darum keine Primzahl. Sie bildet aber mit Dezimalstellen zusammen eine wichtige Prim-Endziffer und ergibt oft selbst Primzahlen, z.B. 19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229 239, 269, 349, 359, 379, 389 und unbegrenzt viele andere!

Die 9er-Zahlenreihe, die sich durch das Tietken-Castell-Register ziehen wird, beginnt mit 9 * 3 (= 27) und wird mit der 9 als konstantem Faktor und den anderen, bei allen Zahlenreihen gleichen ungeraden Faktoren (neben 3, die 5, 7, 9, 11, 13, 15, 17, 19 und unbegrenzt so weiter) die ersten Zahlen der 9er-Reihe bilden.

Da die Einerstelle 9 keine Primzahl ist, koennen keine fuer die Kryptographie benoetigten "grossen Zahlen" gebildet werden, obwohl die gezaehlten zweiten Faktoren 11, 13, 17, 19, 23, 29 und 31 Primzahlen sind und sich dafuer geeignet haetten. Diese Ausgangssituation aendert sich aber im Zusammenhang mit Dezimalstellen. Schon ab den o.g. 19, 29, 59, 79, 89, 109 usw. ist die Prim-Endziffer 9 als Teil von Primzahlen wieder im Rennen.

k)
<u>Resumee aus der 1. Zeile:</u>

Bereits bei diesen o.g. nur 4 Beispielen ist zu sehen, dass die Faktoren (soweit sie vorhanden sind) eine regelmaessige Reihenfolge einhalten. Auf der einen Seite Zahlen mit immer den gleichen Endziffern in der gleichen Reihenfolge (1, 3, (5), 7, 9) und auf der anderen Seite stets die gleichen ungeraden Zahlen in 2er-Schritten kardinal hochgezaehlt.

l)
<u>2. Zeile, 1. bis 5. Zahl: 11 bis 19</u>

Die 2. Zeile berechnet sich, genauso wie alle unbegrenzten weiteren Zeilen, wie die 1. Zeile.

(1)
11 wird mit 3, 5, 7, 9,11 usw.multipliziert. Bei der Multiplikation mit sich selbst ergeben 11 * 11 = 121 (d.h. eine "grosse Zahl"), danach setzt die 11 ihre Reihe mit 11 * 13, 11 * 15, 11 * 17, 11 * 19, 11 * 21 usw. unbegrenzt fort. Fuer eine Verschluesselung waere es hier nicht noetig, eine Primzahl wie 11 mit sich selbst zu multiplizieren, da die anderen Primzahlen bekannt sind, um auch mit denen zusammen eine "grosse Zahl" zu bilden.

(2)
13 wird mit 3, 5, 7, 9, 11,13 usw.multipliziert. Bei der Multiplikation mit sich selbst ergeben 13 * 13 = 169 (d.h. eine "grosse Zahl"), danach setzt die 13 ihre Reihe mit 13 * 15, 13 * 17, 13 * 19, 13 * 21, 13 * 23 usw. unbegrenzt fort. Fuer eine Verschluesselung waere es hier nicht noetig, eine Primzahl wie 13 mit sich selbst zu multiplizieren, da die anderen Primzahlen bekannt sind, um auch mit denen zusammen eine "grosse Zahl" zu bilden.

(3)
15 wird mit 3, 5, 7, 9, 11, 13, 15, 17, 19 usw. multipliziert, kann aber niemals eine "grosse Zahl" fuer die RSA-Kryptographie mit erschaffen, da sie nur als Einerziffer (5) prim ist.

(4)

17 wird mit 3, 5, 7, 9, 11,13, 15, 17 usw.multipliziert. Bei der Multiplikation mit sich selbst ergeben 17 * 17 = 289 (d.h. eine "grosse Zahl"), danach setzt die 17 ihre Reihe mit 17 * 18, 17 * 19, 17 * 21, 17 * 21, 17 * 23 usw. unbegrenzt fort. Fuer eine Verschluesselung waere es hier nicht noetig, eine Primzahl wie 17 mit sich selbst zu multiplizieren, da die anderen Primzahlen bekannt sind, um auch mit denen zusammen eine "grosse Zahl" zu bilden.

(5)
19 wird mit 3, 5, 7, 9, 11,13, 15, 17, 19 usw.multipliziert. Bei der Multiplikation mit sich selbst ergeben 19 * 19 = 361 (d.h. eine "grosse Zahl"), danach setzt die 19 ihre Reihe mit 19 * 21, 19 * 23, 19 * 25, 19 * 27, 19 * 29 usw. unbegrenzt fort. Fuer eine Verschluesselung waere es hier nicht noetig, eine Primzahl wie 19 mit sich selbst zu multiplizieren, da die anderen Primzahlen bekannt sind, um auch mit denen zusammen eine "grosse Zahl" zu bilden.

(6)
21 wird mit 3, 5, 7, 9, 11,13, 15, 17, 19, 21 usw.multipliziert. Bei der Multiplikation mit sich selbst ergeben 21 * 21 = 441 (d.h. eine "grosse Zahl"), danach setzt die 21 ihre Reihe mit 21 * 23, 21 * 25, 21 * 27, 21 * 29, 21 * 31 usw. unbegrenzt fort.

m)
Resumee der 1. bis unbegrenzt "letzten" Zeile:

Die oben gezeigten Faktoren beweisen die Ordnung, Berechenbarkeit und Richtigkeit dieses Tietken-Castell-Prim-Algorithmus.
Es werden bei diesem Tietken-Castell-Prim-Algorithmus fuer die Erkennung, ob bei einer mehr oder weniger zufaellig gefundenen oder unzuverlaessig errechneten Zahl eine Primzahl vorliegt, keine der anfangs genannten komplizierten und unzuverlassigen Verfahren angewendet.

Wenn in einer Zeile, hier z.B. der dritten Zeile, die 21 und 27 zu sehen sind, so ist aus der ersten Zeile bekannt, dass die 21 zur 3er-Reihe gehoert aus 3 * 7 (oder in Additionsform geschrieben: Zur 3 + 6 + 6+ 6) und die 27 zur 9-er Reihe gehoert aus 3 * 9 (oder in Additionsform geschrieben: 9 + 18).
Zu den Zahlen 23 und 29 der gleichen (hier dritten) Zeile aber fuehren keine Faktoren.

n)
Die Abstaende:

Fuer den Algorithmus kann es eine Erleichterung sein, nur addieren zu muessen. Denn es faellt auf, dass die Abstaende wegen der ersten Multiplikation mit sich selbst (d.h. einer Multiplikation mit 2) zwischen allen Zahlen einer Reihe gleich bleiben.
Er bildet immer genau zweimal den ersten Zaehlfaktor. Insofern koennte der Algorithmus nach der ersten Multiplikation die folgenden Zahlen in einer Zahlenreihe auch per Addition der immer gleichen Abstaende bilden.

(1) 3 bildet zu 9 den Abstand 6. Somit folgen nach dieser 9 die Zahlen 15 (9=6), 21 (=15+6), 27 (21+6), 33, 39, 45, 51, 57, 63, 69, 75 und immer so weiter.
(2) 5 vergroessert sich in 10er-Schritten (aus 2 * 5).
(3) Das Gleiche gilt fuer 7. Die Abstaende der Zahlen in dieser Zahlenreihe werden 2 * 7 = 14 betragen (49, 63, 77, 91, 105, 119 usw.).

Zusammenfassung

Rechts von allen Zahlen stehen in dieser Graphik die Faktoren, die abrufbare Hinweise auf ihre spaeteren Produkte geben. Der Algorithmus speichert diese.
Links von diesen spaeteren Produkten werden ihre Faktoren noch einmal notiert, um den Bezug zu ihnen zu demonstrieren.

Primzahlen haben, wie jetzt bekannt, auf ihrer linken Seite keine Hinweise auf Faktoren. Allerdings sagt bei dieser Teilliste, die nur den Weg der 3 zeigt, also noch unvollsstaendig ist, das Fehlen von links der Zahl stehenden Faktoren noch nichts darueber aus, um welche Art von Zahl es sich handelt (Primzahl, "grosse Zahl" oder einfaches Produkt).

Es gibt auch hier am Anfang des Registers bereits viele Doppelbelegungen bei einzelnen Zahlen, d.h. sich ueberschneidende Zahlenreihen, z.B. treffen sich die 3er-Reihe mit 3*21 und die 7er-Reihe mit 7*9 in der Zahl 63. Im zweiten Fall (7 * 9) wuerde sich die 63 als "grosse Zahl" eignen.
(Es waere zu pruefen, ob solche Ueberschneidungen von mehreren Faktorenpaaren in 1 Zahl die kryptographische Sicherheit einer "grossen Zahl" nicht erhoeht, da sie weniger eindeutig zu faktorisieren ist)

A)
Die ersten 120 Zahlen unter Beruecksichtigung nur der 3er-Reihe:

1 3(3*3=9) **5**(3*5=15) **7**(3*7=21) (3*3=9)**9**(3*927)
11(3*11=33)**13**(3*13=39) (3*5=15)**15**(3*15=45) **17**(3*17=51) **19**(3*19=57)
(3*7=21)**21**(3*21=63) **23**(3*23=63**)** **25**(3*25=75)(3*9=27)**27**(3*27=81) **29**(3*2=87)
31(3*31=93)(3*11=33)**33**(3*33=99)**35**(3*35=105)**37**(3*37=111)(3*13=39)**39**(3*117)
41(3*41=123) **43**(3*43=129) (3*15=45)**45**(3*45=135) **47**(3*47=141) **49**
(3*17=51)**51**(3*51=153) **53**(3*53=159) **55**(3*55=165) (3*19=57)**57**(3*57=171) **59**(3*59=177)
61(3*61=183) (3*21=63)**63**(3*63=189) **65**(3*65=195) **67**(3*67=201) (3*23=69) **69**(3*69=207)
71(3*71=213) **73**(3*73=219) (3*25=75)**75**(3*75=225) **77**(3*77=231) **79**(3*79=237)
(3*27=81)**81**(3*81=243) **83**(3*83=249) **85**(3*85=255) (3*29=87)**87**(3*87=261) **89**(3*89=267)
91(3*91=273) (3*31=93)**93**(3*93=279) **95**(3*95=285) **97**(3*97=291) (3*33=99)**99**(3*99=297)
101(3*101=303) **103**(3*103=309) (3*35=105)**105**(3*105=315) **107**(3*107=321)
109(3*109=327)
(3*37=111)**111**(3*111=333) **113**(3*113=339)
115(3*115=345)(3*117=351)**117**(3*117=351)**119**(3*119=357)
121(3*121=363)(3*41=123) **123**(3*123=369) **125**(3*125=375) **127**(3*127=381)
(3*43=129)**129**(3*129=387)
131(3*131=393) **133**(3*133=399) (3*45=135)**135**(3*135=405) **137**(3*137=411)
139(3*139=417)
(3*47=141)**141**(3*141=423) **143**(3*143=429)**145**(3*145=435) (3*49=147)**147**(3*147=441)
149(3*149=447)

B)
Die ersten 120 Zahlen unter Beruecksichtigung nur der 5er-Reihe:
(keine Prim-Endziffer, aber ungerade. Abstaende in 10er-Schritten):

1 **3**(5*3=15) **5**(5*5=25) **7**(5*7=35) **9**(5*9=45)
11(5*11=55) **13**(5*13=65) (5*3=15) **15**(5*15=75) **17**(5*17=85) **19**(5*19=95)
21(5*21=105) **23**(5*23=115) (5*5=25)**25**(5*25=125) **27**(5*27=135) **29**(5*29=145)
31(5*31=155) **33**(5*33=165) (5*7=35)**35**(5*35=175) **37**(5*37=185) **39**(5*39=195)
41(5*41=205) **43**(5*43=215) (5*9=45)**45**(5*45=225) **47**(5*47=235) **49**(5*49=245)
51(5*51=255) **53**(5*53=265) (5*11=55)**55**(5*55=275) **57**(5*57=285) **59**(5*59=295)
61(5*61=305) (7*9=63)**63**(5*63=315) (5*13=65)**65**(5*65=325) **67**(5*67=335) **69**(5*69=345)
71(5*71=355) **73**(5*73=365) (5*15=75)**75**(5*75=375) (7*11=77)**77**(5*77=385) **79**(5*79=395)
81(5*81=405) **83**(5*83=415) (5*17=85)**85**(5*85=425) (5*29=87)**87**(5*87=435) **89**(5*89=445)
(7*13=91)**91**(5*91=455) **93**(5*93=465) (5*19=95)**95**(5*95=475) **97**(5*97=485) **99**(5*99=495)
101(5*101=505) **103**(5*103=515) (5*21=105)**105**(5*105=525) **107**(5*107=535)
109(5*109=545)
111(5*111=555) **113**(5*113=565) (5*23=115)**115**(5*115=575) **117**(5*117=585)
119(5*119=595)
121(5*121=605) **123**(5*123=615) (5*25=125)**125**(5*125=625) **127**(5*127=635)
129(5*129=645)
131(5*131=655) **133**(5*133=665) (5*27=135)**135**(5*135=675) **137**(5*137=685)
139(5*139=695)
141(5*141=705) **143**(5*143=715) (5*29=145)**145**(5*145=725) **147**(5*147=735)
149(5*149=745)

C)
Die ersten 120 Zahlen unter Beruecksichtigung nur der 7er-Reihe:

1 **3**(7*3=21) **5**(7*5=35) **7**(7*7=49) **9**(7*9=63)
11(7*11=77) **13**(7*13=91) **15**(7*15=105) **17**(7*17=119) **19**(7*19=133)
(7*3=21)**21**(7*21=147) **23**(7*23=161) **25**(7*25=175) **27**(7*27=189) **29**(7*29=203)
31(7*31=217) **33**(7*33=231) (7*5=35)**35**(7*35=245) **37**(7*37=259) **39**(7*39=273)
41(7*41=287) **43**(7*43=301) **45**(7*45=315) **47**(7*47=329) (7*7=49)**49**(7*49=343)
51(7*51=357) **53**(7*53=371) **55**(7*55=385) **57**(7*57=399) **59**(7*59=413)
61(7*61=427) (7*9=63)**63**(7*63=441) **65**(7*65=455) **67**(7*67=469) **69**(7*69=483)
71(7*71=497) **73**(7*73=511) **75**(7*75=525) (7*11=77)**77**(7*77=539) **79**(7*79=553)
81(7*81=567) **83**(7*83=581) **85**(7*85=595) (7*29=87)**87**(7*87=609) **89**(7*89=623)
(7*13=91)**91**(7*91=637) **93**(7*93=651) **95**(7*95=665) **97**(7*97=679) **99**(7*99=693)
101(7*101=707) **103**(7*103=721) (7*15=105)**105**(7*105=735) **107**(7*107=749)
109(7*109=763)
111(7*111=777) **113**(7*113=791) **115**(7*115=805) **117**(7*117=819)
(7*17=119)**119**(7*119=833)
121(7*121=847) **123**(7*123=861) **125**(7*125=875) **127**(7*127=889) **129**(7*129=903)
131(7*131=917) (7*19=133)**133**(7*133=931) **135**(7*135=945) **137**(7*137=959)
139(7*139=973)

141(7*141=987) **143**(7*143=1001) **145**(7*145=1015) (7*21=147)**147**(7*147=1029)
149(7*149=1043)

D)

Die ersten 120 Zahlen unter Beruecksichtigung nur der 9er-Reihe:

1 **3**(9*3=27) **5**(9*5=45) **7**(9*7=63) **9**(9*9=81)
11(9*11=99) **13**(9*13=117) **15**(9*15=135) **17**(9*17=153) **19**(9*19=171)
21(9*21=189) **23**(9*23=207) **25**(9*25=225) (9*3=27)**27**(9*27=243) **29**(9*29=261)
31(9*31=279) **33**(9*33=297) **35**(9*35=315) **37**(9*37=333) **39**(9*39=351)
41(9*41=369) **43**(9*43=387) (9*5=45) **45**(9*45=405) **47**(9*47=423) **49**(9*49=441)
51(9*51=459) **53**(9*53=477) **55**(9*55=495) **57**(9*57=513) **59**(9*59=531)
61(9*61=549) (9*7=63)**63**(9*63=567) **65**(9*65=585) **67**(9*67=603) **69**(9*69=621)
71(9*71=639) **73**(9*73=657) **75**(9*75=675) **77**(9*77=693) **79**(9*79=711)
(9*9=81)**81**(9*81=729) **83**(9*83=747) **85**(9*85=765) **87**(9*87=783) **89**(9*89=801)
91(9*91=819) **93**(9*93=837) **95**(9*95=855) **97**(9*97=873) (9*11=99)**99**(9*99=891)
101(9*101=909) **103**(9*103=927) **105**(9*105=945) **107**(9*107=963) **109**(9*109=981)
111(9*111=999) **113**(9*113=1017) **115**(9*115=1035) (9*13=117)**117**(9*117=1053)
119(9*119=1071)
121(9*121=1089) **123**(9*123=1107) **125**(9*125=1125) **127**(9*127=1143) **129**(9*129=1161)
131(9*131=1179) **133**(9*133=1197) (9*15=135)**135**(9*135=1215) **137**(9*137=1233)
139(9*139=1251)
141(9*141=1269) **143**(9*143=1287) **145**(9*145=1305) **147**(9*147=1323) **149**(9*149=1341)

ad A) bis D)

Kommentar zu den obigen vier Tabellen:

Die Prim-Endziffer 1 entfaellt als Faktor. Wuerde sie als Faktor verwendet werden, betraefe sie zwar saemtlich Zahlen des Registers, ohne deren Zahlenwert zu veraendern, aber die Primzahlen waeren durch dieses "1 * 3", "1 * 7", "1 * 9", "1 * 11", "1 * 13" usw. Produkte und verloeren Ihren Status als Primzahlen.
Die Zahlenreihen beginnen also mit der 3, gefolgt von der 7, 9, 11, 13, 15, 17, 19, 21 und unbegrenzt so weiter.
Die drei, bis jeweils 119 reichenden, Tabellen (die eigentlich eine einzige Tabelle ist, die Darstellung in drei Teilen wurde wegen der Uebersichtlichkeit gewaehlt) zeigen, wie nur allein schon die 3-er, 7er- und 9er-Zahlenreihen das Register mit Informationen fuer die Zahlen 3 bis 119 fuellen. Es gibt keine Zahl darin, ueber die keine ausreichenden Informationen ueber die hier zu klaerenden Fragen erhaelt.

Schlussbemerkung: Als Nebeneffekt koennte sich bei entsprechend grossem Register das Faktorisieren von "grossen Zahlen" (d.h. von Produkten aus Prim-Faktoren) eruebrigen. (Der Algorithmus fuer dieses Faktorisieren, der CASTELL-FACT-ALGORITMUS, wurde

bereits im Oktober 2019 von uns gefunden).

Die klein-geschriebene Multiplikation rechts der Zahlen betrifft Informationen fuer spaetere Zahlen.
Die klein-geschriebenen Multiplikation auf der linken Seite einer jeden nicht-Primzahl betrifft die Faktoren, die "von links kommen" und das vorliegende Produkt per Multiplikation erstellt haben.
Diese Faktoren haben, falls sie prim sind, bei der vorliegenden Zahl eine "grosse Zahl" erstellt, die fuer die RSA-Kryptographie benoetigt werden kann, sie sind beim Faktorisieren aber auch gleichzeitig die gesuchten Primzahlen, die hier mitgeliefert werden.

Nikolaus Graf zu Castell-Castell
Dipl. Vw. (Universitaet Hamburg)

Tom Hermann Tietken
MUDr. (Karls-Universitaet Prag)

Prague Research Institute
Zug (CH) und Prague (CR)
mob. 00420 778 037 633
fix line 00420 226 223 026