**Nikolaus Nikolaus Castell-Castell**

**Prague Research Institute**

**Zug (CH) und Prag (CR)**

28.03.2020

**RSA, PGP, Bitcoin & Co.**

**20 Teil-Überlegungen, ausschliesslich mit Multiplikation und Division ein zusammengesetztes Produkt in seinen Primfaktoren zu zerlegen.**

**Ueberlegung 13.**

**Die Frage "Aus welchen Summanden setzt sich die Summe “5” zusammen?" veranlasst die folgenden Versuche 13 bis 18, in denen die grosse Zahl (die Summenzeile, der large integer) versuchsweise von links nach rechts abgearbeitet werden soll.**

**Es ist nicht moeglich, unter den Summanden die zwei “richtigen” fuer die Summe z.B. “5” zu ermitteln**

Jede nicht-triviale Zahl (groesser 1) ist im Sinne der Addition teilbar (2 + 3 = 5). Nicht “teilbar” im Sinne einer Division zu sein (wie es sich z.B. bei den Primzahlen verhaelt) bedeutet lediglich, dass die vorliegende Zahl auf der gezaehlten Faktorenseite nicht in gleich-grosse Teile zerlegbar ist. So bedeutet z.B. 2 \* 3 (von rechts nach links) dass auf der gezaehlten Seite nicht genuegend 2-er Gruppen zur Verfuegung stehen, um sie 3-mal komplett herzustellen, was in diesem Beispiel eine “6” benoetigt und keine “5”.

Wenn, wie in diesem letzten Beispiel, nach der Subtraktion aller Uebertraege (einschliesslich der Mittelteile, d.h. der Ziffern aller Zeilen mit Ausnahme der 1. und letzten Zeile) in der 3. Spalte eine Summenziffer von “4” uebrig bleibt (aus der Einerziffer der 1. bereinigten “8” plus der Einerziffer der 1-

stelligen “6” in der letzten Zeile), dann kann diese “4” gemaess vorangegangener Verfahren des Hochzaehlens nicht “4”, “14”, “24” usw. sein, ausser der “0”, nur 24, 54, 84 und 114 in der zuletzt vorgestellten Liste.

Diese fuer das Faktorisieren nuetzliche Einschraenkung wird allerdings dadurch aufgehoben, dass die “114” einmal, die “24” zweimal und die “54” und “84” je dreimal vorkommen, dass es also in der Liste 10 Antworten auf die Frage nach den Summanden fuer die Summenziffer “4” gibt. Damit behauptet sich auch bei dieser Frage wieder das Dezimalsystem mit seiner unerbittlichen Konsequenz: Was auch in diesen 13 Aufsaetzen an Loesungsversuchen fuer eindeutige Antworten versucht wird, immer wieder ergeben sich statt einer klaren Antwort 10 (ggf. 10 \* 10 Periode) alternative Moeglichkeiten.

Aehnlich verhaelt es sich bei den anderen Summenziffern (0 – 9), deren “1” fuer 21, 51, 71 und 81, deren “2” fuer 12, 42 und 72, deren “3” fuer 3, 33 und 63, deren “5” fuer 15, 45 und 75, deren “6” fuer 6, 36 und 66, deren “7” fuer 27, 57 und 87, deren “8” fuer 18, 48 und 78, deren “9” fuer 9, 39 und 69 und deren “0” fuer 30, 60 und 90 stehen, da sich alle vorgenannten Zahlen in 30-er-Schritten fortsetzen (vgl. “24”, “54”, “84”). Ansonsten gilt fuer alle diese o.g. Summen, dass sie zu einer Art verlaengerter “3-er-Reihe” gehoeren, die wegen der hoeheren Zahlenwerte der “9-er-Reihe” Summen bildet, die ueber 30 hinausreichen. In dieser (begrenzten) Tabelle ergeben sich Summen von 12 bis 120.

In der Praxis des problemlos vorzunehmenden Faktorisierens verbleibt also “nur” die Schwierigkeit, dass die beiden Zahlen der ersten und der letzten Zeile in der (z.B.) 3. Spalte bisher nicht von irgendwoher verlaesslich, mit minimalem Aufwand und eindeutig ableitbar waren.

Aufgrund der Schwierigkeit genau dieses letzten Punktes laesst sich also wiederholend feststellen: Das Thema “Faktorisieren grosser Zahlen” laesst vermuten, dass die zu erwartenden Schwierigkeiten beim Faktorisieren selbst oder in der “grossen Zahl” (wieviel-stellig ist sie und wie immense viele Rechenvorgaenge werden noetig sein?) liegen. Nichts von alledem hat sich in der hier vorliegenden Arbeit bestaetigt. Wie anfangs behauptet, waren bis jetzt fuer den sog. CASTELL-fact-Algorithmus nur die Grundrechnungsarten mit einfachsten Zahlenbeispielen und mit einem Minimum an elementarer “Sprachlogik” noetig, um auf alle hier beschriebenen Loesungen noetig, um auf die hier beschriebenen Loesungsmoeglichkeiten des Faktorisierens grosser Zahlen einfach zu beschreiben.

Tatsaechlich gab und gibt es also bei dem Faktorisieren grosser Zahlen nur das eine Problem hier zum Schluss nur noch das eine Problem, welche 2 (in Bezug auf ein gegebenes konkretes Beispiel) richtigen Summandenziffern in einer gegebenen und vorher von Uebertragen bereinigten Summenziffer enthalten sind.

Im hier zuletzt benutzten Beispiel waren diese 2 Einerziffern “8” und “6” und ergaben die Summenziffer “4” (ganzzahlig “24” aus 18 + 6).

**Ein weiterer Versuch, die oben gestellte Frage nach den 2 gesuchten Summanden zu beantworten**

Es scheint immer klarer zu werden, dass von der “rechten” Seite, d.h. von der bisher erfolgten Berechnung (die in diesem Fall von rechts nach links verlief), keine Hinweise ableitbar waren, die die gesuchten beiden naechsten Spaltenziffern (der ersten und der letzten Zeile) und die zwei daraus abgeleiteten neuen Faktorziffern lieferten.

Nach der “Logik” gibt es nun noch die Moeglichkeit, auf der linken Seite der grossen Zahl zu forschen. Logisch spricht ohnehin eine Rueck-Abwicklung fuer eine Vertauschung von Reihenfolge und Richtung. Wurde von oben rechts nach unten links multipliziert, sollte eine umgekehrte Abwicklung von links unten nach rechts oben vorteilhaft sein.

Um sich das Multiplizieren zu veranschaulichen, sollen in diesem Beispiel weitere Zaehlfaktoren, die weitere tiefer liegende und jeweils seitlich nach links versetzte Zeilen bilden und die die Summenzeile (die “grosse Zahl”) unuebersichtlicher machen, weggelassen werden. Wenn die kleinen Einzelprodukte aus dem einen konstanten zaehlenden Faktor mit den unterschiedlichen, von rechts nach links befindlichen Ziffern des mehrstelligen gezaehlten Faktors, gesondert und untereinander hingeschrieben werden, sodass sich ihre Dezimalstellen nicht in den Einerziffern des naechsten Produkts zur Linken verbergen koennen, dann muessen sie auch bei jeder neuen Zahl um eine Stelle nach links versetzt werden, da die Ziffern des gezaehlten Faktors groessenmaessig von rechts nach links jedes mal um eine Dezimalstelle hoeher liegen.

**Beispiel:**

7 6 4 3 \* 9 =

2 7

3 6

5 4

6 3

= 6 8 7 8 7

Dieses einfache Beispiel laesst einen Einblick in das Wesen der Multiplikation zu und zeigt, wie eindeutig eine Interpretation, die alternativ von rechts nach links vorgenommen wird, sein koennte:

Die in der Summenzeile links unten stehende “6” ist ein Uebertrag, der sich bei dieser Darstellungsart in keiner Einerstelle zu Linken “verstecken” kann. Sie steht in der 5. Spalte allein, weil hier die grosse Zahl mit den insgesamt 5 Stellen der beiden Faktoren endet. Tatsaechlich ist sie die Dezimalstelle von einer noch unbekannten Zahl. Da es sich hier aber bei allen Produkten um Produkte aus der 9-er-Reihe handelt, ist diese 6 die Dezimalstelle von “63” (womit die Faktoren 7 \* 9 klar sind).

Die Summanden der rechts folgenden Summenziffer “8” sind ebenfalls leicht zu finden. Denn die “3” wurde ja soeben schon als Einerziffer der “63” bestimmt, und die “5” ergibt sich aus der Differenz der Summenziffer “8” zu dieser “3”.

Diese “5” ist ebenfalls eine Dezimalstelle und kann in einer 9-er-Reihe nur “54” bedeuten. Mit der “4” in “54” ist nun auch eine der beiden Einerstellen in der naechsten Spalte zur Rechten bekannt und es kann mithilfe der Summenziffer “7” der 2. Summand dieser 3. Spalte ermittelt werden, die “3”.

Diese “3” ist aber wiederum ein Uebertrag von der rechten Spalte, naemlich die Dezimalziffer von “36”, die einzig moegliche Zahl aus der 9-er-Reihe mit einer “3” als Zehnerstelle.

Wie oben laesst sich nun mittels der Summe “8” und dem bereits bekannten Summanden “6” die “2” finden. Damit ist auch die in saemtlichen 12 Aufsaetzen immer wieder unbeantwortete Frage, ob sich in der 1. Spalte ein Uebertrag ergeben hat (oder mit dem Zaehler \* 1 gerechnet werden muss) und welche Hoehe dieser eventuelle Uebertrag hat, beantwortet. Hier ist es die “2”, aus 3 \* 9 = **2**7.

**Ist es doch moeglich, unter zwei Summanden die zwei “richtigen” einer Summe zu ermitteln?**

Es spricht einiges dafuer, die Faktorisierungen (auf der Basis der hier vorliegenden Darlegungsweise) von links unten zu beginnen, zumal nicht nur die bei der von-rechts-oben vorgenommenen Rechnung wichtigen ersten Zeile komplett vorliegt, sondern auch die letzte Zeile. Konkret liegen bei z.B. 2.000 Stellen der grossen Zahl die erste Zeile ca. 1.000 mal vor (so oft, wie der zaehlende Primfaktor Zaehlziffern hat), da diese Stellen (wie in den vorigen Aufsaetzen beschrieben) untereinander und seitlich versetzt immer wieder in gleicher Reihenfolge ihrer Ziffern vorkommen (lediglich pro Zeile mit einem Zaehlfaktor “verfaelscht”).

Somit ist es schwieriger, die Uebertraege von der linken Seite aus zu erkennen, weil sie sowohl bei den Einerziffern als auch bei den Summenziffern “nicht zu sehen” sind. Von “rechts oben” kommend, sind sie zwar auch nicht zu sehen, aber leichter nachzuvollziehen.

7643 \* 9 =

3 \* 9 = **2**7

4 \* 9 = 36 + **2** = **3**8

6 \* 9 = 54 + **3** = **5**7

7 \* 9 = 63 + **5** = 68 usw.

Ausserdem sind bei dieser Rechnungsweise die Einerziffern innerhalb der Spalte errechenbarbar und entscheiden darueber, ob ein entsprechende Summenuebertrag verursacht wird.

Die Frage, wie zwei 1-stellige, bereinigte, Summanden (wie z.B. “4” und “1” aus 54 und 21) in einer Spalte mit der ausgewiesenen Summenziffer “5” (hier genauer mit der “75”) oben die hierfuer erstellte, aber nicht ausreichend eindeutige, Tabelle im Aufsatz 12. Teil, erkennbar sind, muss also immer noch gestellt werden.

**Der neue Weg: Ein Kompromiss**

Wegen der Uebertraege zwischen den Spalten scheint es also unerlaessslich zu sein, die Berechnungen nicht mehr von rechts nach links, sondern von links nach rechts vorzunehmen.

Die stets von rechts kommenden Uebertraege werden naemlich in den Einerziffern der Spalte zur Linken nicht benoetigt. Hier verfaelscht sich dadurch nur die Einerziffer und erschwert das Faktorisieren in dieser Spalte. Auch die Zahl, von der dieser Uebertrag aus der rechts liegenden Spalte kam, kann nicht ohne ihren Uebertrag, der (falls existent) ihre Dezimalstelle war, faktorisiert werden.

Das Problem ist, dass beim Multiplizieren diese Uebertraege von rechts nach links weitergegeben werden, sodass man sie nicht erfassen kann, wenn man “von rechts kommt”, geht man ihnen aber entgegen und muessen sie nicht mehr von der rechten Seite aus geraten werden (wie dies schon bei der (von rechts rechnend) 1. Spalte der Fall war, als es unklar blieb, ob z.B. eine “7” eine 1 \* 7 bedeutet oder eine 3 \* 9 = “27”).

Uebertragen auf das hier schon bekannte, einfache, Beispiel 7643 \* 6719 laesst sich veranschaulichen, wie klar und eindeutig das Rechnen mit Uebertraegen sein kann, wenn man die Summenzeile von links nach rechts abarbeitet und nicht mehr von rechts nach links.

Da in dem diesem Beispiel (und in allen anderen) das Finden nur allein der 1. Zeile oben ausreicht, stellt sich hier die Frage, ob es ausreicht, irgendwo in der Mitte bzw. in der linken Haelfte der grossen Zahl in die Rechnung einzusteigen, denn, wie auch schon dieses kleine Beispiel klar zeigt, endet die 1. Zeile (auf ihrer linken Seite. Das heisst, man kann auch sagen: Beginnt sie) immer vor dem linken Ende der grossen Zahl.

Und wie dieses kleine Beispiel ebenfalls klar zeigt, gibt es Probleme, die grosse Zahl vollstaendig von links abarbeiten zu wollen. Denn hier sind es wieder die Uebertraege , die den Unterschied der Reihenfolge von rechts nach links ausmachen. Waehrend die 1. Spalte rechts ganz klar und eindeutig immer nur eine Ziffer (hier war es die “7”) zeigt, sind die ersten Spalten auf der linken Seite der grossen Zahl unklar. Schon die 1. Ziffer der grossen Zahl (von links) kann aus einem oder zwei Summanden bestehen. Diese koennen 1-stellige Produkt-Ergebnisse sein, aber auch frei stehende Dezimalstellen (Uebertraege), und beide koennen uebereinander zum Stehen kommen oder auch nicht. Aber auch weil die ersten oberen Zeilen an dieser Stelle laengst zu Ende sind, laesst sich nicht klar aussagen, wieviele Ziffern in diesen linken Spalten vorkommen. Letzteres ist allerdings eindeutig moeglich, wenn die Faktorisierungen von der rechten Seite aus beginnen.

Wenn man, von links rechnend, bei keiner einzigen der linken Summenziffern die Gewissheit hat, wieviele Summanden sich in der jeweiligen Spalte uebereinander befinden, ist auch ein Herausrechnen der Mittelteile unmoeglich.

Letzteres aendert sich erst ab der Spalte (hier im Beispiel waere diese Spalte die 4. von links bzw. die 5. von rechts), in der erstmalig eine Ziffer (hier der Uebertrag “6”) der 1. Zeile auftaucht. Im Idealfall ist sie die (immer von rechts gezaehlt) letzte Ziffer links der ersten Zeile.

Ab jetzt wieder im heimischen Bereich der rechten Seite mit seinen beiden Prim-Endziffern zu sein (hier in diesem Beispiel sind es die PE-Ziffer “9”, die diese erste Zeile zu einer 9-er-Reihe macht und die PE-Ziffer “3”, die alle neu hinzukommenden Zeilen mit ihren “3-er-Kopfen” praktisch zu einer (diagonal verlaufenden) 3-er-Reihe macht) hat die bekannten Vorteile: Die Verwendung der vier Prim-Endziffern aus den beiden “letzten” (hier genannt: Ersten) Ziffern der beiden gesuchten mehrstelligen Primfaktoren ergibt eine kleinere Anzahl von Moeglichkeiten und eine groessere Erkennbarkeit, Berechenbarkeit und durch die Wiederholungen der immer gleichen Produkte Vertrautheit.

Diese erste Zeile sollte sich genauso, wie es von der rechten Seite aus versucht worden war, auch von links ausgehend berechnen lassen. Das Instrumentarium hierfuer wurde in den Aufsaetzen Teil 1 – 12 entwickelt.

Allerdings ist wegen der Zeilen dazwischen (z.B.2.000) nicht damit zu rechnen, den linken Anfang der obersten Zeile zu finden, die Faktoren zu erkennen usw.

Unter diesem Aspekt kann auch gleich von Anfang an ganz links unten der grossen Zahl angefangen werden. Dieses funktioniert mit den bereits fuer das Anfangen rechts oben entwickelten Methoden. Die Unterschiede zwischen dem Anfangen rechts oben und links unten sind gering und betreffen v.a. die Positionen und Bedeutungen der Uebertraege zwischen den Spalten und das Fehlen der hilfreichen Prim-Endziffern beim Beginnen links unten. Dafuer entfallen diverse Methoden, die fuer das Anfangen rechts oben entwickelt worden sind (“Rechenschieber”, Doppelreihen-Verfahren, der Ansatz mit den 1.000 Anfangsrechnungen u.a.) und die alle nicht die erhoffte Wirkung erbrachten, die beiden letzten Ziffern einer jeden um die Mittelteile bereinigten Spalte, mithilfe der ebenfalls bereinigten Summenziffer verlaesslich zu finden.

Das Anfangen von links unten hat also die beschriebenen Anfangsschwierigkeiten mit den ersten beiden Ziffern (was ist Produkt und was ist Uebertrag? Wo beginnt die erste Zahl in der 1. oder 2. Spalte? Befinden sich in der ersten Spalte ein oder zwei Ziffern?), und die Uebertraege (v.a. von kleineren Dezimalziffern) koennen mehrere alternative Einerziffern aufweisen (z.B. bei dem konstanten Zaehlfaktor “3” die 12, 15 oder 18 und damit dreimal verschiedene Faktorziffern herstellen, hier 3 \* 4, 3\*5 oder 3\*6), aber es hat sich gezeigt, dass das Anfangen von links unten, wobei die grosse Zahl von links aus abgearbeitet wird, unerlaesslich ist, weil es von rechts oben nicht zu funktionieren scheint.

Kleinere, weil selten vorkommende, Nachteile des von links-Rechnens, wie die Tatsache, dass sich z.B. zu einer “2” in einer 3-er-Reihe immer nur die Dezimalstelle “1” hinzufuegen laesst, es aber umgekehrt zwei Wahlmoeglichkeiten gibt (zu einer Dezimalziffer “1” waeren sowohl “2” (12) als auch “8” (18) moeglich u.v.a.) sind in Kauf zu nehmen. Ausserdem kann der Castell-fact-Algorithmus seltene Faelle auffangen und bei Fehlermeldung die gegebenen Alternativen anbieten.

Mit dem anfangs erwaehnten Zahlenbeispiel 7643 \* 9 sollte “Einblick in das Wesen der Multiplikation“ gewonnen werden. Dieser Einblick wurde tatsaechlich gewonnen, indem auch hierbei klar wurde, dass die Faktorisierung von links nach rechts zu erfolgen hat.

**Zahlenbeispiel 7643 \* 6719 (Primzahlen)**

63+5 54+3 36+2

(6) =68 =57 =38 27

---------------------------------------------------------------------------------------------

7 6 4 3

---------------------------------------------------------------------------------------------

49+4 42+3 28+2

(5) =53 =45 =30 21

---------------------------------------------------------------------------------------------

42+3 36+2 24+1

(4) = 45 =38 =25 18

----------------------------------------------------------------------------------------------

**5 1 3 5 3 3 1 7**

1 1 2 2 1 1 (Summenuebertraege)

**Interpretation**

Die “6” ist eine Dezimalstelle in der 5. Spalte, die in der ersten 9-er-Reihe fuer die 4. Spalte nur die Einerziffer “3” moeglich macht. Die entstandene 63 ergibt die Faktoren 7 mit dem konstanten Faktor 9 und laesst mittels der Summenziffer, die zuvor von den Zahlenwerten der Mittelteile 6 und 30 befreit wurde, nur die untere Ziffer “8” zu. Diese ergibt als Mitglied, weniger der Reihe des konstanten Zaehlers “6”, als vielmehr der 3-er-Kopf-Reihe, eine “18”.

Nun muessten die beiden uebrig gebliebenen Zahlen (6)3 und (1)8 die Summenziffer (8)1 ergeben. Da die Summenziffer aber (8)6 aufweist, ist der Uebertrag (“5”) gefunden, der aus der oberen Spaltenzahl (6)3 eine (6)8 gemacht hat. Er wird als Dezimalstelle in die 3. Spalte (gezaehlt von rechts) zurueckgereicht und bildet dort innerhalb der 9-er-Reihe die Zahl (5)4.

Nach Herausrechnung des einen Mittelteils (“4”) kann die 2. Ziffer (aufgrund der um den Mittelteil “4” und den Summenuebertrag “1” bereinigten Summenziffer, also Summenziffer 10 - 5 = 5) nur eine “1” sein und als Teil der 3-er-Reihe eine 21 ergeben. Da die Summenziffer aber nicht “5” anzeigt, sondern “8” (aus 13 – 5), ist die Differenz “3” und somit als Uebertrag von rechts “entlarvt”.

Dieser Uebertrag stellt fuer die obere Ziffer die Dezimalstelle dar, womit die obere Zahl nur eine 36 und die untere Zahl (Summenziffer 9 – 6 = 3) nur eine 3 sein kann.

Da die Summenziffer allerdings nicht 6 + 3 = 9 betraegt, sondern (1)1, ist die Differenz “2” als Dezimalstelle fuer die 7 in der ersten Spalte zum ersten mal klar und muss nicht “geraten” werden.

**Zusammenfassung der Handhabungen beim Rechnen von links nach rechts**

1)

Die Klaerung der Frage: Gibt es eine Summenziffer von rechts nach links, die zuerst aus der 1. Summenziffer der grossen Zahl links heraus-subtrahiert werden muss? Diese ist nicht sichtbar, sondern muss vorerst geraten werden (in der Mitte der grossen Zahl ist sie logischerweise am groessten: Es ist die Stelle, an der sich die unterste und oberste Zeile entweder mit ihren Enden treffen oder sich ueberschneiden).

Nach Herausrechnung der Mittelteile entscheidet der Zahlenwert der beiden verbleibenden Einerziffern darueber, ob es einen Summenuebertrag nach links gibt und wie hoch dieser ist. Die Einerziffern der beiden Summanden “4” und “5” z.B. ergeben keinen Uebertrag in die Spalte links. Die Ziffern “4” und “6” aber wuerden die 2-stellige Summe “10” erreichen und ergaeben einen Summen-Uebertrag von rechts nach links.

Waeren die Zeilen in der hier vorliegenden Form tatsaechlich sichtbar, bedeutete eine ungerade Spaltenanzahl, dass es sich bei der Ziffer in der 2. Spalte ganz links um einen Uebertrag handelt. Dies zu wissen, ist nuetzlich, denn, wenn es ein Uebertrag ist, steht dieser ganz links in einer zusaetzlichen Spalte, und es kann keine Ziffer darueber geben, selbst wenn die Zeile darueber ebenfalls eine zusaetzliche Spalte mit einem Uebertrag aufweist.

2)

Koennte schon vorher gewusst weden, wie hoch der Zahlenwert der Faktoren einer Zeile ist, waere mit dieser Kenntnis die Bestimmung moeglich, ob es sich bei der ersten Ziffer ganz links um einen Uebertrag handelt oder um ein Produkt, ggf. mit einer Ziffer darueber, die einen Uebertrag in ihrer Zeile darstellt.

Wuerde es sich bei der Ziffer in der 1. Spalte ganz links um ein Produkt handeln, waeren deren Faktoren relative klein, weil sich dann die hier moeglichen Multiplikationen im Einerbereich befinden muessten (z.B. bei “4” = 1\*4 oder 2 \* 2). Waeren hoehere Multiplikatoren im Spiel (wie z.B. 2 \* 7 = 14), muesste sich eine Spalte weiter links auch noch diese Dezimalstelle “1” als Uebertrag zeigen.

Aber, ob vorher erkennbar oder nicht, es ist immer nur der Zahlenwert der Faktoren, der darueber entscheidet, ob eine Zeile an ihrer ersten Stelle mit einem Uebertrag beginnt (so wuerde z.B. 6 \* 1 keinen Uebertrag nach links hin verursachen, 6 \* 2 aber wohl).

Darueber, ob es auch unten in der grossen Zahl Uebertraege gibt, entscheidet der Zahlenwert der Einerstellen der Produkte in den Spalten. Sie sind unabhaengig von der Groesse der Faktoren (vgl. die grossen Faktoren 9 \* 9 ergeben 81, also nur eine “1” als Summand in den Spalten).

Im Falle eines Uebertrags in der 1. Spalte links (hier z.B. “4”) stellt diese 1. Spalte der 1. Zeile unten keine Spalte dar, in der die 1. Faktorisierung stattfinden kann (z.B. 42 = 6 \* 7). Diese kann erst in der 2. Spalte vorgenommen werden, in der es oft auch einen Uebertrag gibt, der zur 2. Zeile (von unten gezaehlt) gibt (hier die “5”).

Es waere also nicht hilfreich, bereits den 1. Uebertrag in der 1. Spalte (hier “4” in die Faktoren 2 \* 2) zu faktorisieren.

3)

Nachdem z.B. die “4” aus der 1. Spalte als Uebertrag identifiziert ist und als Dezimalstelle in der 2. Spalte Verwendung findet, taucht das erwaehnte Problem einer ungenauen Zuordnung auf. Die Dezimalstelle “4” z.B. kann mindestens fuenf Einerstellen (40, 42, 45, 48, 49) haben, die alle unterschiedliche Faktoren ergaeben (8 \* 5, 7 \* 6, 9 \* 5, 6 \* 8, 7 \* 7).

Um die richtige Einerziffer zu ermitteln (hier die “2” fuer 42), muessten die konstanten Faktoren (hier 7 \* 6) oder die zweite oben liegende Ziffer (hier “5”) bereits bekannt sein. Diese 5 ist ihrerseits ein Uebertrag, der in der 3. Spalte dem Produkt 49 (aus 7 \* 7) plus Uebertrag “4” = **5**3 zur Dezimalziffer “5” verhilft und als gesamtes Produkt (53) im naechsten Moment als Mittelteil fuer immer verschwinden wird.

Diese obere 5 in der 2. Spalte ist nicht leicht zu errechnen, denn die Summenziffer “1” in der 2. Spalte setzt sich nicht nur einfach aus oben 5 und unten 2 zusammen, sondern es kommen auch noch eine Summenzifer “1” hinzu und unten ein Uebertrag von “3” (42 + 3 = 45). Alle diese genannten Ziffern stehen miteinander in Verbindung und koennen voneinander hergeleitet werden. Die Reihenfolge hierfuer muss vorher festgelegt sein.

4)

Ab der fertig gestellten 2. Ziffer wird es einfach, da ab jetzt die zwei wichtigsten Faktoren (der konstante Zaehlfaktor der ersten Zeile unten, hier die “6”, und der konstante Faktor aller ersten Stellen einer jeden, sich oben neu bildenden, Zeile (der sog. “Koepfe”, hier die “7”) bekannt sind und als erste Massnahme bei der Bearbeitung einer neuen Spalte zuerst einmal die zahlenmaessig sukzessiv anwachsenden Mittelteile mit den von der vorigen Spalte schon bekannten Faktoren (nebst ihren Uebertraegen) herausgerechnet werden.

Diese Herausrechnung erfolgt mit den “bereinigten” Zahlen, insofern haben die Uebertraege bei der Berechnung der Mittelteile keine Bedeutung. Sie muss nur insofern beruecksichtigt werden, als dass die Uebertraege die Summenziffern vergroessern und darum ebenfalls aus den Summenziffern herausgerechnet werden muessen. Dies gilt auch fuer den in der zweiten Spalte oben befindlichen Uebertrag “5”. Er muss von der Summenziffer “1” subtrahiert werden. Somit betraegt die Summenziffer abzueglich dem Summenuebertrag “1” und dem obigen Spaltenuebertrag “5” nur noch “5”.

Diese “5” aus 45 setzt sich aber aus dem Produkt 42 und dem Uebertrag “3” zusammen. Wenn die 42 aus den beiden Faktoren (hier Zeile 6 und Koepfe 7) klar ist, laesst sich aus der Differenz zwischen 42 und 45 die “3” als Uebertrag fuer die Spalte 3 der ersten Zeile errechnen.

Welche Ziffern, hier z.B. der 1. Spalte, zuerst verlaesslich feststehen (z.B. die Summenziffer ”1” und der Uebertrag aus der 1. Spalte) und welche Ziffern sich in welcher Reihenfolge voneinander ableiten, muss beim Algorithmus festgelegt sein.

Das Ende der 1. Zeile wird sich mitten in der grossen Zahl befinden und u.a. dadurch gekennzeichnet sein, dass es mit den Kopffaktoren der ersten Zeile oben rechts (hier der konstanten “3”) Kontakt bekommt.

Da die 1. Zeile oben und die 1. Zeile unten die gleiche Zeile ist, ist die letzte Zahl der unteren Zeile die gleiche wie die 1. Zahl der oberen Zeile (hier 27 aus 3 \* 7). Die Kopfziffer wird ebenfalls “3” sein, nur der Zaehlfaktor wird mit 90%-iger Wahrscheinlichkeit nicht noch einmal “7” sein. Im konkret vorliegenden Beispiel betraegt der konstante Faktor fuer die 1. Zeile unten “6”.

**Nachwort**

Wenn der Aufwand der hier vorliegenden 12 Aufsatz-Teile bedacht wird, mit denen in alle Richtungen erfolglose Versuche unternommen wurden, ueber die 2. Ziffer der grossen Zahl hinauszukommen, dann muesste dieser letzte neue Versuch hier in diesem 13. Teil des Aufsatzes die vorigen Bemuehungen als Irrungen und Wirrungen und verlorene Zeit und Muehe aussehen lassen.

Andererseits scheinen aber gerade die vorgenannten vielfaeltigen Bemuehungen zu allen moeglichen Details die Voraussetzungen geschaffen haben, so vertraut mit den benoetigten einfachen Zahlen und den hier hingehoerenden Fragen zu werden, dass innerhalb weniger Tage das “eigentliche” Problem des Faktorisierens (naemlich einfach nur zwei Summanden in einer Summe benennen zu koennen!) erkannt und innerhalb eines Tages prinzipiell geloest werden konnte.

**Nikolaus Graf zu Castell-Castell**

**Dipl. Vw.**

**Prague Research Institute**

**Zug (CH) und Prague (CR)**

**Nikolaus.Castell@mail.com**

**mob. 00420 778 037 633**