Theoreme über die in dieser Form $paa \pm qbb$ enthaltenen Teiler von Zahlen*

Leonhard Euler

In den folgenden Lehrsätzen bezeichnen die Buchstaben a und b irgendwelche ganzen zueinander teilerfremden Zahlen oder solcher, die außer der Einheit keinen anderen gemeinsamen Teiler haben.

Theorem 1

Alle Primteiler der in der Form $aa + bb$ enthaltenen Zahlen sind entweder 2 oder Zahlen von der Form $4m + 1$.

Theorem 2

Alle Primzahlen der Form $4m + 1$ sind umgekehrt in der Form von Zahlen $aa + bb$ enthalten.

Theorem 3

Also kann die Summe von zwei Quadraten oder eine Zahl der Form $aa + bb$ nicht durch eine Zahl der Form $4m - 1$ geteilt werden.

*Originaltitel: "Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum", zuerst publiziert in: *Commentarii academiae scientiarum Petropolitanae, Band 14* (1751, geschrieben 1747): pp. 151 – 181, Nachdruck in: Opera Omnia: Serie 1, Band 2, pp. 194 – 222, Eneström Nummer E164, übersetzt von: Alexander Aycock für den "Euler-Kreis Mainz".

Theorem 4

Alle Primteiler der in dieser Form $aa + 2bb$ enthaltenen Zahlen sind entweder 2 *oder in der Form* $8m + 1$ *oder* $8m + 3$ *enthaltene Zahlen.*

Theorem 5

Alle in der Form $8m + 1$ *oder* $8m + 3$ *enthaltenen Primzahlen sind umgekehrt Zahlen der Form* $aa + 2bb$.

Theorem 6

Keine Zahl der Form $aa + 2bb$ *kann durch eine Zahl der Form* $8m - 1$ *oder* $8m - 3$ *geteilt werden.*

Theorem 7

Alle Primteiler der in der Form $aa + 3bb$ *enthaltenen Zahlen sind entweder* 2 *oder* 3 *oder in einer der Formen* $12m + 1$, $12m + 7$ *enthalten.*

Theorem 8

Alle in einer beiden Formen $12m + 1$ *oder* $12m + 7$ *oder in dieser einen* $6m + 1$ *enthaltenen Primzahlen sind zugleich Primzahlen der Form* $aa + 3bb$.

Theorem 9

Keine Zahl der Form $12m - 1$ *oder* $12m - 7$, *das heißt, keine Zahl der Form* $6m - 1$, *ist ein Teiler einer in der Form* $aa + 3bb$ *enthaltenen Zahl.*

Theorem 10

Alle Primteiler von in der Form $aa + 5bb$ *enthaltenen Zahlen sind entweder* 2 *oder* 5 *oder in einer der* 4 *Formen* $20m + 1$, $20m + 3$, $20m + 7$, $20m + 9$ *enthalten.*

THEOREM 11

Wenn die Zahlen $20m+1$, $20m+3$, $20m+9$, $20m+7$ *prim waren, dann wird es sein wie folgt:*

$$20m+1 = aa+5bb, \quad 2(20m+3) = aa+5bb,$$
$$20m+9 = aa+5bb, \quad 2(20m+7) = aa+5bb.$$

THEOREM 12

Keine in einer der folgenden Formen enthaltene Zahl $20m-1$, $20m-3$, $20m-9$, $20m-7$ *kann ein Teiler einer Zahl der Form* $aa+5bb$ *sein.*

THEOREM 13

Alle Primteiler der in der Form $aa+7bb$ *enthaltenen Zahlen sind entweder* 2 *oder* 7 *oder in einer der folgenden*

sechs Formeln		oder in einer dieser drei
$28m+1$,	$28m+11$,	$14m+1$,
$28m+9$,	$28m+15$,	$14m+9$,
$28m+25$,	$28m+23$	$14m+11$

enthalten.

THEOREM 14

Wenn die in diesen Formen $14m+1$, $14m+9$, $14m+11$ *Zahlen prim sind, dann sind sie zugleich in der Form* $aa+7bb$ *enthalten.*

THEOREM 15

Keine Zahl der Form $aa+7bb$ *kann durch eine Zahl geteilt werden, die in einer der folgenden*

sechs Formeln		oder diesen drei
$28m + 3$,	$28m + 5$,	$14m + 3$,
$28m + 13$,	$28m + 17$,	$14m + 5$,
$28m + 19$,	$28m + 27$	$14m + 13$

enthalten ist.

THEOREM 16

Alle Primteiler der in der Form $aa + 11bb$ enthaltenen Zahlen sind entweder 2 *oder* 11 *oder in einer der folgenden*

10 *Formeln*		*oder* 5 *Formeln*
$44m + 1$,	$44m + 3$,	$22m + 1$,
$44m + 9$,	$44m + 27$,	$22m + 3$,
$44m + 37$,	$44m + 23$,	$22m + 9$,
$44m + 25$,	$44m + 31$,	$22m + 5$,
$44m + 5$,	$44m + 15$,	$22m + 15$

enthalten.

THEOREM 17

Wenn die in diesen entweder zehn oder fünf Formeln enthaltenen Zahlen prim sind, dann werden sie zugleich entweder entweder sie selbst oder des Vierfache Zahlen der Form $aa + 11bb$ sein.

THEOREM 18

Keine Zahl der Form $aa + 11bb$ kann durch eine der Zahlen geteilt werden, welche in einer der folgenden

10 *Formeln*		oder 5 *Formeln*
$44m+7$,	$44m+29$,	$22m+7$,
$44m+13$,	$44m+35$,	$22m+13$,
$44m+17$,	$44m+39$,	$22m+17$,
$44m+19$,	$44m+41$,	$22m+19$,
$44m+21$,	$44m+43$,	$22m+21$

enthalten ist.

THEOREM 19

Alle Primteiler der in der Form $aa+13bb$ *enthaltenen Zahlen sind entweder* 2 *oder* 3 *oder in einer der folgenden* 12 *Formen*

$$\begin{array}{ll}
52m+1, & 52m+7,\\
52m+49, & 52m+31,\\
52m+9, & 52m+11,\\
52m+25, & 52m+19,\\
52m+29, & 52m+47,\\
52m+17, & 52m+15.
\end{array}$$

enthalten.

THEOREM 20

Alle Primzahlen, die in der ersten Spalte dieser Formeln enthalten sind, sind zugleich von der Form $aa+13bb$. *Aber das Doppelte dieser Primzahlen, welches in der anderen Spalte von Formeln enthalten sind, sind Zahlen der Form* $aa+13bb$.

THEOREM 21

Keine Zahl der Form $aa + 13bb$ kann durch eine Zahl geteilt werden, die in einer der folgenden Formeln enthalten ist:

$$\begin{array}{ll} 52m + 3, & 52m + 35, \\ 52m + 5, & 52m + 37, \\ 52m + 21, & 52m + 41, \\ 52m + 23, & 52m + 43, \\ 52m + 27, & 52m + 45, \\ 52m + 33, & 52m + 51. \end{array}$$

THEOREM 22

Alle Primteiler der in der Form $aa + 17bb$ enthaltenen Zahlen sind entweder 2 oder 17 oder in einer der folgenden Formeln enthalten:

$$\begin{array}{ll} 68m + 1, & 68m + 3, \\ 68m + 9, & 68m + 27, \\ 68m + 13, & 68m + 39, \\ 68m + 49, & 68m + 11, \\ 68m + 33, & 68m + 31, \\ 68m + 21, & 68m + 63, \\ 68m + 53, & 68m + 23. \end{array}$$

THEOREM 23

Alle Primzahlen, die in der ersten Spalte dieser Formen enthalten sind, zu welchen 2 hinzugezählt werden muss, sind von der Form $aa + 17bb$, oder sie selbst oder deren Neunfaches. Aber die Dreifachen der in der anderen Spalte enthaltenen Primzahlen sind Zahlen der Form $aa + 17bb$.

THEOREM 24

Keine Zahl der Form $aa + 17bb$ kann durch eine Zahl geteilt werden, die in eine der folgenden Formen enthalten ist.

$$\begin{array}{ll} 68m - 1, & 68m - 3, \\ 68m - 9, & 68m - 27, \\ 68m - 13, & 68m - 39, \\ 68m - 49, & 68m - 11, \\ 68m - 33, & 68m - 31, \\ 68m - 25, & 68m - 7, \\ 68m - 21, & 68m - 63, \\ 68m - 53, & 68m - 23. \end{array}$$

THEOREM 25

Alle Primteiler von in der Form $aa + 19bb$ enthaltenen Zahlen sind entweder 2 oder 19 oder in einer der folgenden

$$\begin{array}{llcl} \multicolumn{2}{c}{18 \textit{ Formen}} & & \textit{oder dieser } 9 \textit{ Formen} \\ 76m + 1, & 76m + 5, & & 38m + 1, \\ 76m + 25, & 76m + 49, & & 38m + 5, \\ 76m + 17, & 76m + 9, & & 38m + 7, \\ 76m + 45, & 76m + 73, & & 38m + 9, \\ 76m + 61, & 76m + 7, & & 38m + 11, \\ 76m + 35, & 76m + 23, & & 38m + 17, \\ 76m + 39, & 76m + 43, & & 38m + 23, \\ 76m + 63, & 76m + 11, & & 38m + 25, \\ 76m + 55, & 76m + 47, & & 38m + 35 \end{array}$$

enthalten.

THEOREM 26

Alle Primzhalen, die in einer dieser Formeln enthalten sind, sind entweder sie selbst oder viermal genommen Zahlen der Form $aa + 19bb$.

THEOREM 27

Keine Zahl der Form $aa + 19bb$ kann durch eine Zahl geteilt werden, die in eine der folgenden 9 Formen enthalten ist:

$$\begin{array}{lll} 38m - 1, & 28m - 9, & 38m - 23, \\ 38m - 5, & 28m - 11, & 38m - 25, \\ 38m - 7, & 28m - 17, & 38m - 35. \end{array}$$

In diesen Lehrsätzen ist Natur der Formen $aa + qbb$ enthalten, wenn q eine Primzahl war; und zuerst haben wir freilich gesehen, dass alle Primteiler von Formen dieser Art entweder 2 oder q sind oder in solchen Ausdrücken $4qm + \alpha$ so erfasst werden können, dass kein Teiler in ihnen nicht enthalten ist, dann aber, dass jede Primzahl $4qm + \alpha$ zugleich ein Teiler der einer gewissen Form $aa + qbb$ ist. Weiter lässt sich aber auch erschließen, wenn eine Primzahl der Form $4qm + \alpha$ ein Teiler einer gewissen Zahl $aa + qbb$ war, dass dann keine Zahl der Form $4qm - \alpha$ ein Teiler desselben Ausdrucks $aa + qbb$ sein kann. Weil also unter den Formen der Teiler der Formel $aa + qbb$ immer dieser $4mq + 1$ enthalten ist, ist es offenkundig, dass keine Zahl $aa + qbb$ durch eine Zahl der Form $4mq - 1$ geteilt werden kann. Schließlich wird dem aufmerksamen Leser klar werden, wenn q eine Primzahl der Form $4n - 1$ war, dass dann die Formen der Teiler auf eine halb so kleine Zahl reduziert werden können, sodass sie auf die Formeln $2qm + \alpha$ zurückgeführt werden können, was nicht geschehen kann, wenn q eine Primzahl der Form $4n + 1$ ist. Wenn also für diese Form $aa + (4n + 1)bb$ ein Teiler $4(4n + 1)m + \alpha$ war, dann wird keine Zahl von dieser Form

$$4(4n + 1)m + 2(4n + 1) + \alpha$$

ein Teiler desselben Ausdrucks $aa + (4n + 1)bb$ sein können. Wir wollen mehrere Anmerkungen machen, nachdem wir auch die Formen $aa + qbb$, wannimmer q keine Primzahl ist, betrachtet haben werden.

THEOREM 28

Alle Primteiler von in der Form $aa + 6bb$ oder $2aa + 3bb$ enthaltenen Zahlen sind entweder 2 oder 3 oder in einer der folgenden Formen enthalten

$$\begin{array}{ll} 24m + 1, & 24m + 7, \\ 24m + 5, & 24m + 11. \end{array}$$

THEOREM 29

Alle Primzahlen der Form $24m + 1$ oder $24m + 7$ sind in dem Ausdruck $aa + 6bb$ enthalten; aber die Primzahlen, die die Form $24m + 5$ oder $24m + 11$ haben, sind im Ausdruck $2aa + 3bb$ enthalten.

THEOREM 30

Keine Zahl der Form $aa + 6bb$ oder $2aa + 3bb$ kann durch keine Zahl geteilt werden, die in einer dieser Formen enthalten ist

$$\begin{array}{ll} 24m - 1, & 24m - 5, \\ 24m - 7, & 24m - 11. \end{array}$$

THEOREM 31

Alle Primteiler von in dieser Form $aa + 10bb$ oder dieser Form $2aa + 5bb$ enthaltenen Zahlen sind entweder 2 oder 5 oder in einer der folgenden Formen enthalten

$$
\begin{aligned}
&40m + \ \ 1, \quad 40m + \ \ 7,\\
&40m + \ \ 9, \quad 40m + 23,\\
&40m + 11, \quad 40m + 37,\\
&40m + 19, \quad 40m + 13.
\end{aligned}
$$

THEOREM 32

Die in der ersten Spalte dieser Formeln enthaltenen Primzahlen sind zugleich Zahlen von dieser Form $aa + 10bb$*; und die in der anderen Spalte enthaltenen Primzahlen sind Zahlen der Form* $2aa + 5bb$*.*

THEOREM 33

Keine Zahl der Form $aa + 10bb$ *oder dieser* $2aa + 5bb$ *kann durch eine Zahl geteilt werden, die in einer der folgenden Formeln enthalten ist*

$$
\begin{aligned}
&40m - \ \ 1, \quad 40m - \ \ 7,\\
&40m - \ \ 9, \quad 40m - 23,\\
&40m - 11, \quad 40m - 37,\\
&40m - 19, \quad 40m - 13.
\end{aligned}
$$

THEOREM 34

Alle Primzahlen von in der Form $aa + 14bb$ *oder* $2aa + 7bb$ *enthaltenen Zahlen sind entweder* 2 *oder* 7 *oder in einer der folgenden Formen enthalten*

$$\begin{array}{ll}
56m+\ \ 1, & 56m+\ \ 3,\\
56m+\ \ 9, & 56m+27,\\
56m+25, & 56m+19,\\
56m+15, & 56m+\ \ 5,\\
56m+23, & 56m+45,\\
56m+39, & 56m+13.
\end{array}$$

THEOREM 35

Die in der ersten Spalte dieser Formen enthaltenen Primzahlen sind zugleich Zahlen der Form $aa + 14bb$ *oder* $2aa + 7bb$*; aber erst das Dreifache derer, die aber in der anderen Spalte enthalten sind, werden in der anderen Spalte dieser Formen erfasst.*

THEOREM 36

Wenn in den obigen Formeln die Zeichen $+$ *oder* $-$ *verändert werden, dann wird keine in diesen Formen enthaltene Zahl ein Teiler der Form* $aa + 14bb$ *oder* $2aa + 7bb$ *sein.*

THEOREM 37

Alle Primteiler von in der Form $aa + 15bb$ *oder* $3aa + 5bb$ *enthaltenen Zahlen sind entweder* 2 *oder* 3 *oder* 5 *oder in einer der folgenden Formeln*

$$\begin{array}{llcl}
 & & & \textit{oder dieser } 4\\
60m+\ \ 1, & 60m+31, & & 30m+\ \ 1,\\
60m+17, & 60m+47, & & 30m+17,\\
60m+19, & 60m+49, & & 30m+19,\\
60m+23, & 60m+53 & & 30m+23.
\end{array}$$

enthalten.

THEOREM 38

Alle Primteiler von in der Form $aa + 21bb$ oder $3aa + 7bb$ enthaltenen Zahlen sind entweder 2 oder 3 oder 7 oder in einer der folgenden Formeln enthalten

$$\begin{array}{ll}
84m + 1, & 84m + 5, \\
84m + 25, & 84m + 41, \\
84m + 37, & 84m + 17, \\
84m + 55, & 84m + 11, \\
84m + 31, & 84m + 23, \\
84m + 19, & 84m + 71.
\end{array}$$

THEOREM 39

Alle Primteiler von in der Form $aa + 35bb$ oder $5aa + 7bb$ enthaltenen Zahlen sind entweder 2 oder 5 oder 7 oder in einer der folgenden Formeln *oder dieser*

$$\begin{array}{lll}
140m + 1, & 140m + 3, & 70m + 1, \\
140m + 9, & 140m + 27, & 70m + 3, \\
140m + 81, & 140m + 103, & 70m + 9, \\
140m + 29, & 140m + 87, & 70m + 11, \\
140m + 121, & 140m + 83, & 70m + 13, \\
140m + 109, & 140m + 47, & 70m + 17, \\
140m + 11, & 140m + 33, & 70m + 27, \\
140m + 99, & 140m + 17, & 70m + 29, \\
140m + 51, & 140m + 13, & 70m + 33, \\
140m + 39, & 140m + 117, & 70m + 39, \\
140m + 71, & 140m + 73, & 70m + 47, \\
140m + 79, & 140m + 97, & 70m + 51.
\end{array}$$

enthalten.

THEOREM 40

Alle Primteiler von in einer der Formen

$$\begin{array}{ll}
aa + 30bb, & 2aa + 15bb, \\
3aa + 10bb, & 5aa + 6bb
\end{array}$$

enthaltenen Zahlen sind entweder 2 *oder* 3 *oder* 5 *oder in einer der folgenden Formen enthalten*

$$\begin{aligned}
&120m + 1, \quad 120m + 11,\\
&120m + 13, \quad 120m + 23,\\
&120m + 49, \quad 120m + 59,\\
&120m + 37, \quad 120m + 47,\\
&120m + 17, \quad 120m + 67,\\
&120m + 101, \quad 120m + 31,\\
&120m + 113, \quad 120m + 43,\\
&120m + 29, \quad 120m + 79.
\end{aligned}$$

Diese Lehrsätze genügen, um die folgenden Bemerkungen zu formulieren, aus welchen die Natur von Teilern von Form der Art $paa + qbb$ umfassender erkannt werden wird.

Bemerkung 1

Die Formel $paa + qbb$ hat keinen Teiler, der nicht zugleich Teiler der Formel $aa + pqbb$ ist. Der Grund für diese Tatsache ist freilich schnell klar; denn welche Zahl ein Teiler der Form $paa + qbb$ ist, wird zugleich auch diese Form $ppaa + pqbb$ teilen, das heißt, diese $aa + pqbb$, nachdem a stelle von pa gesetzt worden ist. Deswegen wird es genügen, diese eine einzige Form $aa + Nbb$ betrachtet zu haben, die natürlich in Bezug auf die Teiler diese $paa + qbb$ in sich umfasst.

Bemerkung 2

Unter den Primzahlen, die eine in der Form $aa + Nbb$ enthaltene Zahl teilen, tritt zwei zuerst auf. Wenn N nämlich eine ungerade zahl ist, wird, indem man für a und b ungerade Zahlen nimmt, die Formel $aa + Nbb$ durch 2 teilbar werden; aber wenn N eine gerade Zahl ist, wird für gerades a die Formel auch durch 2 teilbar. Weiter wird auch die Zahl N oder jeder beliebige echte Teiler von ihr ein Teiler der Formel $aa + Nbb$ sein, was durch Nehmen von $a = N$ offenkundig ist.

Bemerkung 3

Die übrigen Primteiler der Form $aa + Nbb$ können in Ausdrücken von dieser Art $4Nm + \alpha$ erfasst werden, sodass auch umgekehrt alle in der Form $4Nm + \alpha$ enthaltenen Primzahlen zugleich Teiler der Form $aa + Nbb$ sind. Außerdem, wenn der Ausdruck $4Nm + \alpha$ Teiler der Form $aa + Nbb$ liefert, dann wird keine Zahl von dieser Art $4Nm - \alpha$ ein Teiler einer in der Form $aa + Nbb$ enthaltenen Zahl sein können.

Bemerkung 4

α wird aber bestimmte Werte haben, die von der Gestalt der Zahl N abhängen werden; und freilich wird die Einheit immer einer aus den Werten für α sein. Aber dann, weil die Frage von in der Form $4Nm + \alpha$ enthaltenen Primzahlen handelt, ist es offensichtlich, dass weder eine gerade Zahl noch eine Zahl, die ein gemeinsamen Teiler mit N hat, einen Wert von α festlegen kann.

Bemerkung 5

Aber alle Werte von α werden kleiner als $4N$ sein; wenn sie nämlich größer wären, könnten sie durch Vermindern der Zahl m kleiner als $4N$ gemacht werden. Daher werden die Werte von α ungerade Zahlen kleiner als $4N$ und teilerfremd zu N sein. Und in der Tat werden auch nicht alle ungeraden zu N teilerfremden Zahlen geeignete Werte für α darbieten, sondern die Hälfte von ihnen wird von diesem Unterfangen ausgeschlossen, weil ja, wenn x ein Wert für α war, dann $-x$ oder $4N - x$ nicht auch ein passender Wert sein kann; und umgekehrt, wenn x kein Wert für α war, dann wird $4N - x$ gewiss ein Wert für α sein.

Bemerkung 6

Also wird die Anzahl der Werte für α, sodass $4Nm + \alpha$ alle Primteiler der Formel $aa + Nbb$ enthält, auf die folgende Weise bestimmt werden. Es seien p, q, r, s etc. einander verschiedene Primzahlen, zwei ausgenommen, welche getrennt zu betrachten ist, und

wenn galt,	ist die Anzahl der Werte für α
$N = 1$,	1,
$N = 2$,	2,
$N = p$,	$p - 1$,
$N = 2p$,	$2(p - 1)$,
$N = pq$,	$(p - 1)(q - 1)$,
$N = 2pq$,	$2(p - 1)(q - 1)$,
$N = pqr$,	$(p - 1)(q - 1)(r - 1)$,
$N = 2pqr$	$2(p - 1)(q - 1)(r - 1)$
etc.	etc.

BEMERKUNG 7

So wie aber die Einheit immer unter den Werten von α gefunden wird, so muss auch jede ungerade und zu N teilerfremde Quadratzahl unter den Werten von α auftreten. Nachdem nämlich b einfach als gerade Zahl $2c$ festgelegt worden ist, wird die Formel $aa + 4Ncc$ werden, welche, wenn sie eine Primzahl ist, im Ausdruck $4Nm + \alpha$ enthalten sein muss. Also wird α entsprechend aa oder der Rest sein, welcher aus der Teilung von aa durch $4N$ zurückbleibt. In gleicher Weise müssen unter den Werten für α alle Zahlen $aa + N$ gefunden werden oder die, welche aus deren Teilung durch $4n$ als Reste übrigbleiben; nachdem nämlich $b = 2c + 1$ gesetzt worden ist, wird $aa + Nbb = aa + N + 4N(cc + c)$ werden; wenn diese Zahl prim war, wird $aa + N$ ein Wert für α sein müssen.

BEMERKUNG 8

Man sieht aber ein, wenn x ein Wert von α war, dass dann auch xx (was freilich aus dem Vorhergehenden klar ist) und gänzlich alle Potenzen von x, seien sie x^μ, unter der Werten für α auftreten müssen. Wenn weiter außer x auch y ein Wert von α war, dann wird auch xy und allgemein $x^\mu y^\mu$ einen Wert für α geben. Wenn $x^\mu y^\mu$ größer als $4N$ war, teile man durch dieses und der Rest wird ein Wert für α sein. Wenn in gleicher Weise darüber hinaus z ein Wert von α war, dann wird auch $x^\mu y^\mu z^\mu$ ein Wert für α sein. Und daher werden aus einem einzigen oder einigen bekannten Werten für α ohne Mühe ganz und gar alle seine Werte gefunden.

BEMERKUNG 9

Es sei x eine zu $4N$ teilerfremde Zahl und auch kleiner als sie; dann wird entweder x oder $-x$ ein Wert für α sein. Wenn also x eine Primzahl war, wird aus der folgenden Tabelle eingesehen werden, in welchen Fällen $+x$ und in welchen $-x$ einen Wert für α liefert:

Für	ist
$N = 3n - 1$	$\alpha = +3$
$N = 3n + 1$	$\alpha = -3$
$N = \begin{cases} 5n+1 \\ 5n+4 \end{cases}$	$\alpha = +5$
$N = \begin{cases} 5n+2 \\ 5n+3 \end{cases}$	$\alpha = -5$
$N = \begin{cases} 7n+3 \\ 7n+5 \\ 7n+6 \end{cases}$	$\alpha = +7$
$N = \begin{cases} 7n+1 \\ 7n+2 \\ 7n+4 \end{cases}$	$\alpha = -7$

Für	ist
$N = \begin{cases} 11n + 2 \\ 11n + 6 \\ 11n + 7 \\ 11n + 8 \\ 11n + 10 \end{cases}$	$\alpha = +11$
$N = \begin{cases} 11n + 1 \\ 11n + 3 \\ 11n + 4 \\ 11n + 5 \\ 11n + 9 \end{cases}$	$\alpha = -11$

Wenn irgendeine Primzahl vorgelegt ist, wird, ob selbige, mit vorangestellten Vorzeichen $+$ oder $-$, einen Wert für α liefert, so ausfindig gemacht werden: Es müssen zwei Fälle entwickelt werden, der eine, in dem die vorgelegte Primzahl von der Form $4u + 1$ ist, der andere, in dem sie von der Form $4u - 1$ ist. Im ersten Fall wird $\alpha = (4u + 1)$ sein, wenn $N = (4u + 1)n + tt$ war, aber $\alpha - (4u + 1)$, wenn $N \neq (4u + 1)n + tt$ war. Im zweiten Fall wird aber $\alpha = +(4u - 1)$ sein, wenn $N \neq (4u - 1)n + tt$ ist, aber $\alpha = -(4u - 1)$, wenn $N = (4u - 1)n + tt$ ist. Dort ist zu bemerken, wie das Zeichen $=$ eine Gleichheit bezeichnet, dass so das Zeichen $\neq$ die Unmöglichkeit der Gleichheit bedeutet. Wenn aber für jeden der beiden Fälle $N = (4u \pm 1)n + s$ war, wird auch $N = (4u \pm 1)n + s^\nu$, während ν irgendeine ganze Zahl ist, sein, woraus die Tabelle für bestimmte Primzahlen ohne Mühe konstruiert wird.

Bemerkung 10

Weil man ja unter den Formen der Primteiler von $aa + Nbb$ die Zahl $4Nm + 1$ hat, wird derselbe Ausdruck $aa + Nbb$ durch keine Zahl geteilt werden können, die in der Form $4Nm - 1$ enthalten ist. Weil in gleicher Weise $4Nm + tt$ die Form der Teiler des Ausdrucks $aa + Nbb$ darbietet, folgt, dass keine Zahl von dieser Art $4Nm - tt$ ein Teiler einer in der Form $aa + Nbb$ enthaltenen Zahl sein kann, wenn freilich, was ich immer festlege, a und b zueinander teilerfremd sind. Dieser Sache wegen wird diese Gleichung $(4Nm - tt)u = aa + Nbb$ unmöglich sein und daher wird $4Nmu - ttu - Nbb \neq aa$ sein, wenn freilich $4Nmu - ttu$ und Nbb teilerfremde Zahlen waren; weil das gewiss geschieht, wenn $b = 1$ und $t = 1$ ist, erlangen wir diese

Folgerung

Keine in der Form $4abc - b - c$ enthaltene Zahl kann jemals ein Quadrat sein.

Bemerkung 11

Wenn N eine Zahl der Form $4n - 1$ war, dann reduzieren sich die Formen der Teiler auf eine doppelt so kleine Form, sodass sie in den Formeln $2Nm + \alpha$ erfasst werden. Natürlich, wenn die Form der Teiler $4Nm + \alpha$ war, dann wird auch $4Nm + 2N + \alpha$ eine Form der Teiler sein. Weil also $2Nm + tt$ die Form der Teiler ist, folgt, dass keine Zahl $2Nm - tt$ ein Teiler der Form $aa + Nbb$ sein kann. Daher wird $(2Nm - tt)u \neq aa + Nbb$ sein, wobei $N = 4n - 1$ ist, woraus dann dies entspringt:

Folgerung

Keine Zahl der Form $2abc - b - c$, wenn entweder b oder c eine ungerade Zahl $4n - 1$ war, kann jemals ein Quadrat sein.

Annmerkung 12

Wenn N eine ungerade Zahl der Art $4n + 1$ war oder auch eine ungerade gerade Zahl, dann können die Formen der Teiler nicht auf eine doppelt so kleine Zahl reduziert werden. Wenn natürlich $4Nm + \alpha$ ein Teiler der Form $aa + Nbb$ war, dann wird $4Nm + 2N + \alpha$ kein Teiler derselben Form sein können. Daher wird $2(2m + 1)N + tt$ kein Teiler der Form $aa + Nbb$ sein und daher diese Gleichung $(2(2m + 1)N + tt)u = aa + Nbb$ unmöglich, wenn freilich a und b teilerfremd sind und N entweder eine ungerade Zahl der Form $4n + 1$ oder eine ungerade gerade Zahl Zahl ist. Daraus ergibt sich diese

Folgerung

Keine Zahl der Form $2ab - b + c$, während a eine ungerade und b eine ungerade gerade oder ungerade Zahl der Form $4n + 1$ ist, kann jemals ein Quadrat sein.

SCHOLION 1

Was bisher alles gesagt worden ist, zeigt zur Genüge die Natur von Teilern von Formen der Art $aa + Nbb$ auf und dient zugleich zum schnellen Finden aller Formen der Teiler, in Kenntnis von welchen auch die Formen der Zahlen bekannt werden, die niemals Teiler der Form $aa + Nbb$ liefern können. Weil sich also diese Dinge auf alle Werte von N erstrecken, ob sie Primzahlen oder zusammengesetze Zahlen sind, verbleibt es, dass wir auch die Fälle entwickeln, in denen N negative prime und zusammengesetze Zahlen bezeichnet; es ist aber ersichtlich, dass die Formel $paa - qbb$ keinen Teiler haben kann, der nicht zugleich ein Teiler von dieser $aa - pqbb$ oder dieser $pqaa - bb$ ist, woher es genügen wird, nur Formen der Art $aa - Nbb$ entwickelt zu haben.

THEOREM 41

Alle Primteiler von in der Form $aa - bb$ enthaltenen Zahlen sind entweder 2 *oder* $4m \pm 1$*; natürlich ist keine Zahl gegeben, die nicht ein Teiler der Differenz von zwei Quadraten ist. Umgekehrt sind aber alle Zahlen außer den ungerade geraden selbst Differenzen von zwei Quadraten.*

THEOREM 42

Alle Primteiler von in der Form $aa - 2bb$ enthaltenen Zahlen sind entweder 2 *oder von der Form* $8m \pm 1$. *Und alle Primzahlen der Form* $8m \pm 1$ *sind auf unendliche viele Arten in der Form $aa - 2bb$ enthalten.*

THEOREM 43

Alle Primteiler von in der Form $aa - 3bb$ enthaltenen Zahlen sind entweder 2 *oder* 3 *oder von der Form* $12m + \pm 1$. *Und umgekehrt sind alle Primzahlen von dieser Art zugleich in der Form $aa - 3bb$ oder $3aa - bb$ auf unendlich viele Weisen enthalten.*

THEOREM 44

Alle Primteiler der Form $aa - 5bb$ sind entweder 2 *oder* 5 *oder*

in der einen von diesen Formen	*oder in dieser einen*
$20m \pm 1, \quad 20m \pm 9$	$10m \pm 1.$

enthalten. Und alle in diesen Formen enthaltenen Primzahlen sind zugleich Teiler der Form $aa - 5bb$.

THEOREM 45

Alle Primteiler der Form $aa - 7bb$ sind entweder 2 oder 7 oder in einer der folgenden Formen enthalten

$$28m \pm 1, \quad 28m \pm 3, \quad 28m \pm 9;$$

und umgekehrt sind alle in diesen Formen enthaltenen Primzahlen zugleich Teiler der Form $aa - 7bb$.

THEOREM 46

Alle Primteiler der Form $aa - 11b$ sind entweder 2 oder 11 oder in einer der folgenden Formen enthalten

$$44m \pm 1, \quad 44m \pm 5, \quad 44m \pm 7, \quad 44m \pm 9, \quad 44m \pm 19;$$

und umgekehrt sind alle in diesen Formeln enthaltenen Primzahlen zugleich Teiler der Form $aa - 11b$, welche Reziprozität in allen folgenden Theoremen Geltung hat.

THEOREM 47

Alle Primteiler der Form $aa - 13bb$ sind entweder 2 oder 13 oder in den folgenden Formen enthalten

	welche auf diese reduziert werden
$52m \pm 1, \quad 52m \pm 3,$	$26m \pm 1,$
$52m \pm 9, \quad 52m \pm 25,$	$26m \pm 3,$
$52m \pm 23, \quad 52m \pm 17,$	$26m \pm 9.$

THEOREM 48

Alle Primteiler der Form aa $-$ 17*bb sind entweder* 2 *oder* 17 *oder in den folgenden Formen enthalten*

		welche auf diese reduziert werden
$68m \pm 1$,	$68m \pm 9$,	$34m \pm 1$,
$68m \pm 13$,	$68m \pm 19$,	$34m \pm 3$,
$68m \pm 33$,	$68m \pm 25$,	$34m \pm 9$,
$68m \pm 21$,	$68m \pm 15$,	$34m \pm 9$,

THEOREM 49

Alle Primteiler der Form aa $-$ 19*bb sind entweder* 2 *oder* 19 *oder in den folgenden Formen enthalten*

$$\begin{array}{lll} 76m \pm 1, & 76m \pm 3, & 76m \pm 9, \\ 76m \pm 27, & 76m \pm 5, & 76m \pm 15, \\ 76m \pm 31, & 76m \pm 17, & 76m \pm 25. \end{array}$$

THEOREM 50

Alle Primteiler der Form aa $-$ 6*bb sind entweder* 2 *oder* 4 *oder in diesen Formen enthalten*

$$24m \pm 1, \quad 24m \pm 5.$$

THEOREM 51

Alle Primteiler der Form aa $-$ 10*bb sind entweder* 2 *oder* 5 *oder in diesen Formen enthalten*

$$40m \pm 1, \qquad 40m \pm 3,$$
$$40m \pm 9, \qquad 40m \pm 13.$$

THEOREM 52

Alle Primteiler der Form $aa - 14bb$ *sind entweder* 2 *oder* 7 *oder in diesen Formen enthalten*

$$\begin{array}{lll} 56m \pm 1, & 56m \pm 5, & 56m \pm 25, \\ 56m \pm 13, & 56m \pm 9, & 56m \pm 11. \end{array}$$

THEOREM 53

Alle Primteiler der Form $aa - 22bb$ *sind entweder* 2 *oder* 11 *oder in diesen Formen enthalten*

$$\begin{array}{lll} 88m \pm 1, & 88m \pm 3, & 88m \pm 9, \\ 88m \pm 27, & 88m \pm 7, & 88m \pm 21, \\ 88m \pm 25, & 88m \pm 13, & 88m \pm 39, \\ & 88m \pm 29. & \end{array}$$

THEOREM 54

Alle Primteiler der Form $aa - 15bb$ *sind entweder* 2 *oder* 3 *oder* 5 *oder in diesen Formen enthalten*

$$60m \pm 1, \quad 60m \pm 7, \quad 60m \pm 11, \quad 60m \pm 17.$$

THEOREM 55

Alle Primteiler der Form $aa - 21bb$ *sind entweder* 2 *oder* 3 *oder* 7 *oder in den folgenden Formen enthalten* *welche auf diese reduziert werden*

$84m \pm 1$,	$84m \pm 5$,	$42m \pm 1$,
$84m \pm 25$,	$84m \pm 41$,	$42m \pm 5$,
$84m \pm 37$,	$84m \pm 17$,	$42m \pm 17$.

THEOREM 56

Alle Primteiler der Form $aa - 33bb$ sind entweder 2 oder 3 oder 11 oder in den folgenden Formen enthalten

welche auf diese reduziert werden

$132m \pm 1$,	$132m \pm 17$,	$66m \pm 1$,
$132m \pm 25$,	$132m \pm 29$,	$66m \pm 17$,
$132m \pm 35$,	$132m \pm 65$,	$66m \pm 25$,
$132m \pm 49$,	$132m \pm 41$,	$66m \pm 29$,
$132m \pm 37$,	$132m \pm 31$,	$66m \pm 31$.

THEOREM 57

Alle Primteiler der Form $aa - 33bb$ sind entweder 2 oder 3 oder 11 oder in den folgenden Formen enthalten

$140m \pm 1$,	$140m \pm 9$,	$140m \pm 59$,
$140m \pm 29$,	$140m \pm 19$,	$140m \pm 31$,
$140m \pm 13$,	$140m \pm 23$,	$140m \pm 67$,
$140m \pm 43$,	$140m \pm 33$,	$140m \pm 17$.

THEOREM 58

Alle Primteiler der Form $aa - 30bb$ sind entweder 2 oder 3 oder 5 oder in den folgenden Formen enthalten

$$\begin{array}{lll} 120m \pm 1, & 140m \pm 13, & 120m \pm 49, \\ 120m \pm 37, & 140m \pm 7, & 120m \pm 29, \\ 120m \pm 17, & 140m \pm 19. & \end{array}$$

THEOREM 56

Alle Primteiler der Form $aa - 105bb$ sind entweder 2 oder 3 oder 5 oder 7 in den folgenden Formen enthalten

		welche auf diese reduziert werden
$420m \pm 1$,	$420m \pm 13$,	$210m \pm 1$,
$420m \pm 169$,	$420m \pm 97$,	$210m \pm 13$,
$420m \pm 23$,	$420m \pm 121$,	$210m \pm 23$,
$420m \pm 107$,	$420m \pm 131$,	$210m \pm 41$,
$420m \pm 109$,	$420m \pm 157$,	$210m \pm 53$,
$420m \pm 59$,	$420m \pm 73$,	$210m \pm 59$,
$420m \pm 101$,	$420m \pm 53$,	$210m \pm 73$,
$420m \pm 151$,	$420m \pm 137$,	$210m \pm 79$,
$420m \pm 89$,	$420m \pm 103$,	$210m \pm 89$,
$420m \pm 79$,	$420m \pm 187$,	$210m \pm 97$,
$420m \pm 41$,	$420m \pm 113$,	$210m \pm 101$,
$420m \pm 209$,	$420m \pm 197$,	$210m \pm 103$.

Bemerkung 13

Also sind alle Primteiler von in der Form $aa - Nbb$ enthaltenen Zahlen entweder 2 oder Teiler der Zahl N oder werden in Formeln von der Art $4Nm \pm \alpha$ erfasst. Wenn nämlich $4Nm + \alpha$ die Form der Teiler war, dann wird auch $4Nm - \alpha$ eine Form der Teiler sein; aber nicht bei den Formen $aa + Nbb$; wenn $4Nm + \alpha$ ein Teiler von diesen war, dann wird $4Nm - \alpha$ nie einen Teiler derselben Formel liefern können.

Bemerkung 14

Nachdem also $4Nm \pm \alpha$ für die allgemeine Form der Teiler der in dem Ausdruck $aa - Nbb$ enthaltenen Zahlen festgelegt worden ist, wird der Buchstabe α zumeist mehrere Zahlen bedeuten, unter welchen die Einheit sicher immer enthalten ist; aber dann, weil hier die Rede von Primteilern ist, wird unter den Werten von α keine gerade Zahl und auch kein Teiler der Zahl N sein. Weiter ist es auch klar, dass alle Werte für α so aufbereitet werden können, dass sie kleiner als $2N$ sind. Wenn nämlich $4Nm + 2N + b$ ein Teiler ist, dann wird für $m - 1$ anstelle von m gesetzt $4Nm - (2N - b)$ ein Teiler sein. Also werden die Werte für α ungerade zu N teilerfremde Zahlen sein und nur die Hälfte kleiner als $2N$ wird geeignete Werte für α liefern; die übrigen werden Formeln darbieten, in denen überhaupt kein Teiler enthalten ist. Man wird natürlich immer so viele Formen an Teilern haben, wie es Nichtteiler gibt, einzig ausgenommen im Fall $N = 1$.

Bemerkung 16

Sowie aber die Einheit immer unter den Werten für α gefunden wird, so wird auch eine gewisse Quadratzahl, die prim zu $4N$ ist, einen geeigneten Wert für α an die Hand geben. Nachdem nämlich $b = 2c$ gesetzt worden ist, geht die Formel $aa - Nbb$ in $aa - 4Ncc$ oder $4Ncc - aa$ über, woher klar wird, dass jede Quadratzahl aa, welche teilerfremd zu $4N$ ist, einen geeigneten Wert für α darbietet, indem man natürlich den Rest nimmt, welcher bei Division von aa durch $4N$ zurückbleibt. Indem man auf gleiche Weise $b = 2c + 1$ setzt, geht die Formel $Nbb - aa$ in $4N(cc + c) + N - aa$ über, woher auch alle Zahlen $N - aa$ oder $aa - N$, welche freilich prim zu $4N$ sind, geeignete Werte für α liefern werden. Weiter ist auch anzumerken, wenn x, y, z Werte für α sind, dass dann auch x^μ, y^μ, z^μ und ebenso alle Produkte, die aus den Zahlen x, y, z und irgendwelchen Potenzen von ihnen resultieren, Werte für α darbieten werden; daher werden in Kenntnis eines oder einiger Werte von α ohne Mühe gefunden.

Bemerkung 17

Damit aber noch klar wird, Werte von welcher Art der Buchstabe α immer haben wird, scheint es ratsam, die folgende Tabelle beizufügen, ähnlich der, welche man in Bemerkung 9 hat.

Man hat	für
$\alpha = 3$	$N = 3n + 1$
$\alpha \neq 3$	$N = 3n - 1$
$\alpha = 5$	$N = 5n \begin{cases} +1 \\ -1 \end{cases}$
$\alpha \neq 5$	$N = 5n \begin{cases} +2 \\ -2 \end{cases}$
$\alpha = 7$	$N = 7n \begin{cases} +1 \\ +2 \\ -3 \end{cases}$
$\alpha \neq 7$	$N = 7n \begin{cases} -1 \\ -2 \\ +3 \end{cases}$
$\alpha = 11$	$N = 11n \begin{cases} +1 \\ -2 \\ +3 \\ +4 \\ +5 \end{cases}$
$\alpha \neq 11$	$N = 11n \begin{cases} -1 \\ +2 \\ -3 \\ -4 \\ -5 \end{cases}$

$$
\begin{array}{c|c}
\alpha = 13 & N = 13n \begin{cases} +1 \\ -1 \\ +3 \\ -3 \\ +4 \\ -4 \end{cases} \\
\alpha \neq 13 & N = 13n \begin{cases} +2 \\ -2 \\ +5 \\ -5 \\ +6 \\ -6 \end{cases}
\end{array}
$$

BEMERKUNG 18

Aus dieser Tabelle können also die Primzahlen, die geeignete Werte für α liefern, leicht erkannt und die unpassenden verworfen werden. Nachdem nämlich eine Primzahl p vorgelegt worden ist, können alle Quadratzahlen in Formeln der Art $pn + \theta$ erfasst werden, welche hervorgehen, indem man für θ alle Quadratzahlen einsetzt oder die Reste, die aus der Teilung der Quadrate durch p zurückbleiben. Wenn also N eine Zahl der Art $pn + tt$ war, dann wird man unter den Formen der Teiler $4Nm \pm \alpha$ der Formel $aa - Nbb$ oder $Nbb - aa$ entsprechend $\alpha = p$ haben; wenn aber die zahl n nicht in der Form $pn + tt$ enthalten ist, dann wird keine in der Form $4Nm \pm p$ enthaltene Zahl ein Teiler eine Zahl der Form $aa - Nbb$ sein können.

BEMERKUNG 19

Wenn N eine ungerade Zahl der Form $4n + 1$ war, dann können die Formen der Teiler $4Nm \pm \alpha$ des Ausdrucks $aa - Nbb$ auf doppelt so kleine zurückgeführt werden, sodass sie in der Art $2Nm \pm \alpha$ dargeboten werden können. In diesem Fall, wenn $4Nm \pm \alpha$ die Form der Teiler war, wird natürlich auch $4Nm \pm (2N - \alpha)$ eine Form der Teiler sein; und weil im Fall $N = 13$ eine Form der Teiler der Form $aa - 13bb$ ja $52m \pm 3$ war, wird auch $52m \pm 23$ eine Form der Teiler sein.

BEMERKUNG 20

Wenn aber N eine ungerade gerade Zahl oder eine ungerade Zahl der Form $4n-1$ war, dann gelingt diese Reduktion der teilenden Formen auf doppelt so kleine nicht. Wenn in diesem Fall die Form der Teiler des Ausdrucks $aa-Nbb$ also $4Nm \pm \alpha$ war, dann wird $4Nm \pm (2N-\alpha)$ keine solche sein, das heißt: Keine in der Form $2(2m \pm 1)N \pm \alpha$ enthaltene Form wird ein Teiler einer Zahl der Art $aa-Nbb$ sein. Nachdem also $\alpha = tt$ gesetzt worden ist, wird $(2(2m \pm 1)N \pm tt))u \neq aa-Nbb$ sein. Daraus erlangen wir diese

FOLGERUNG

Keine in der Form $2ab \pm c + b$ *enthaltende Zahl kann jemals ein Quadrat sein, wenn freilich a eine ungerade Zahl und b eine ungerade gerade Zahl oder eine ungerade Zahl der Form* $4n-1$ *war.*

SCHOLION 2

Es können unzählige speziellere Formeln dieser Art, die nie ein Quadrat werden können, aus den obigen abgeleitet werden. Wir wollen nämlich die erste Form $aa+Nbb$ betrachten und es sei $4Nm+A$ eine Formel solcher Art, dass keine in ihr enthaltene Zahl ein Teiler der Form $aa+Nbb$ sein kann. Also wird $aa+Nbb \neq (4Nm+A)u$ sein, während mit dem Zeichen $\neq$ eine unmögliche Gleichung bezeichnet wird, woraus $aa \neq 4Nmu + Au - Nbb$ entspringt. Es sei $b = Ac$; es wird

$$aa \neq 4Nmu + Au - NAAcc$$

werden. Man setze weiter $u = NAcc + d$ und es wird $aa \neq = 4NNAmcc + 4Nmd + Ad$ sein. Es sei $d = 4NNn$; es wird $aa \neq 16N^3mn + 4NNAmcc + 4NNAn$ sein. Man teile diese Form durch das Quadrat $4NN$ und setze $c = 1$ und es wird $4Nmn + Am + An$ eine Formel sein, die nie ein Quadrat sein können wird, wenn freilich die Form $aa+Nbb$ nicht durch eine der in der Formel $4Nm+A$ enthaltene Zahl geteilt werden kann. Aus den obigen Lehrsätzen erschließen wir also, dass keine Zahl, die in einem der folgenden Ausdrücke enthalten ist, ein Quadrat werden kann.

$$
\begin{array}{rr}
4mn - (m+n), & 4mn + 3(m+n), \\
8mn - (m+n), & 8mn + 7(m+n), \\
8mn - 3(m+n), & 8mn + 5(m+n), \\
12mn - (m+n), & 12mn + 11(m+n), \\
12mn - 7(m+n), & 12mn + 5(m+n), \\
20mn - (m+n), & 20mn + 19(m+n), \\
20mn - 3(m+n), & 20mn + 17(m+n), \\
20mn - 7(m+n), & 20mn + 13(m+n), \\
20mn - 9(m+n), & 20mn + 11(m+n), \\
24mn - (m+n), & 20mn + 23(m+n), \\
24mn - 5(m+n), & 20mn + 19(m+n), \\
24mn - 7(m+n), & 20mn + 17(m+n), \\
24mn - 11(m+n), & 20mn + 13(m+n), \\
28mn - (m+n), & 28mn + 27(m+n), \\
28mn - 9(m+n), & 28mn + 19(m+n), \\
28mn - 11(m+n), & 28mn + 17(m+n), \\
28mn - 15(m+n), & 28mn + 13(m+n), \\
28mn - 23(m+n), & 28mn + 5(m+n), \\
28mn - 25(m+n), & 28mn + 3(m+n)
\end{array}
$$

etc.

Es ist aber zu bemerken, dass in den Formeln der einen Spalte die Zahlen m und n in Bezug auf den Koeffizienten von $m+n$ prim sein müssen. Diese Einschränkung verlangt die Bedingung, welche wir eingangs gestellt haben, dass in der Form $aa + Nbb$ die Zahlen a und b zueinander teilerfremde Zahlen sind; wenn diese Bedingung nämlich nicht beachtet wird, könnte jede beliebige Zahl ein Teiler dieser Form sein. Im Übrigen ist es unter Beachtung dieser Bedingung aus dem Vorhergehenden klar, wenn $4Nm - A(m+n)$ kein

Quadrat sein kann, dass auch diese sich weiter erstreckende $4Nmn - A(m + n) \pm 4Np(m+n)$ kein Quadrat sein kann.

SCHOLION 3

Wir wollen nun den Ausdruck $aa - Nbb$ betrachten, von welchem kein Teiler in der Form $4Nm \pm A$ enthalten sei. Also wird $aa - Nbb \neq 4Nmu \pm A$ oder $aa \pm 4Nmu + NAA \pm Au$ sein. Man setze $NA \pm u = d$ oder $u = \pm d \mp NA$ und es wird $aa \neq \pm 4Nmd \mp 4NNAm + Ad$ sein. Es sei $d = \pm 4NNn$ und es wird

$$16N^3mn \mp 4NNAm \pm 4NNAn \neq aa$$

werden, woher klar ist, dass keine in der Formel $4Nmn \pm A(m-n)$ enthaltene Zahl ein Quadrat sein kann. Und daher wird auch keine in diesem Ausdruck $4Nmn \pm A(m-n) \pm 4pN(m-n)$ enthaltene Zahl ein Quadrat sein können, wenn nur die zuvor erwähnte Bedingung beachtet wird, dass a und b zueinander prime Zahlen sind. Daher werden aus den letzten Theoremen die folgenden Formeln abgeleitet, die niemals ein Quadrat liefern können:

$$\begin{array}{rr}
8mn \pm 3(m-n), & 8mn \pm 5(m-n), \\
12mn \pm 5(m-n), & 12mn \pm 7(m-n), \\
20mn \pm 3(m-n), & 20mn \pm 17(m-n), \\
20mn \pm 7(m-n), & 20mn \pm 13(m-n), \\
24mn \pm 7(m-n), & 24mn \pm 17(m-n), \\
24mn \pm 11(m-n), & 24mn \pm 13(m-n), \\
28mn \pm 5(m-n), & 28mn \pm 23(m-n), \\
28mn \pm 11(m-n), & 20mn \pm 17(m-n), \\
28mn \pm 13(m-n), & 20mn \pm 15(m-n),
\end{array}$$

etc.

Dem aufmerksamen Leser wird leicht klar werden, dass die beiden Zahlen m und n in Bezug auf die Koeffizienten von $(m-n)$ prim sein müssen; denn andernfalls, wenn in der Formel $12mn \pm 5(m-n)$ beispielsweise $m = 5p$ und

$n = 5q$ gesetzt werden würde, ginge $12 \cdot 25pq \pm 25(p-q)$ hervor und daher könnte diese Formel $12pq \pm (p-q)$ kein Quadrat sein; das ist aber dennoch falsch.