BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
MATHEMATISCH-NATURWISSENSCHAFTLICHE KLASSE

SITZUNGSBERICHTE

JAHRGANG

1957

MÜNCHEN 1958

VERLAG DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN

In Kommission bei der C. H. Beck'schen Verlagsbuchhandlung München

Über die Aufsuchung von Teilern der natürlichen Zahlen

Von Max Schneidt in München

Vorgelegt von Herrn Georg Faber am 8. November 1957

Übersicht

Jede nicht durch 2, 3 und 5 teilbare natürliche Zahl $Z > 1$ läßt sich in die Form bringen

$$Z = 30\,k + c. \tag{1}$$

Die ganze Zahl $k \geqq 0$ heiße der Index der Zahl Z. c bezeichnet eine der acht Primzahlen

$$7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31. \tag{2}$$

Die Zahlen Z ordnen sich derart in acht arithmetische Progressionen. Die Gesamtheit aller Zahlen der Form $30k + c$ mit festem c wird als die Menge M_c bezeichnet. Demgegenüber sei Z_c eine bestimmte Zahl dieser Menge.

k heiße Primzahlindex in bezug auf die Menge M_c, wenn $30k + c$ Primzahl ist.

Die Form

$$N = 2^\alpha\, 3^\beta\, 5^\gamma\, (30k + c)$$

(α, β, γ ganze Zahlen $\geqq 0$) umfaßt alle natürlichen Zahlen, auch die nur durch 2, 3 und 5 teilbaren, wenn man für $k = 0$ noch $c = 1$ zuläßt.

Im folgenden wird mehrfach an Stelle der Form $30k + 31$ die Form $30k + 1$ verwendet. Es lassen sich dann die acht Zahlen

c viermal paarweise zur Summe 30 zusammenfassen. Die Menge M_{31} ist mit der Menge M_1 identisch, wenn $k = 0$ in M_1 ausgeschlossen wird.

Die Euklid'sche Zahl $(2.3.5).7.11.13.17 \ldots\ldots P + 1$, wo P eine beliebig hohe Primzahl bedeutet, gehört der Menge M_1 an.

Ebenso die 4. Potenz von $30k + c$, da $c^4 \equiv 1 \bmod 30$.

Die Zahl $10^n + 1$ gehört der Menge M_{11} an, da $10^n - 10$ durch 30 teilbar ist.

Es ist

$$2^7 \equiv 8 \bmod 30 \text{ und } 2^8 \equiv 16 \bmod 30.$$

Daher ist $2^{4n+3} - 1 \equiv 7 \bmod 30$, und die Lucas'sche Primzahl $2^{127} - 1$ gehört der Menge M_7 an.

Da $2^{4n} + 1 \equiv 17 \bmod 30$, so gehören alle Gauß'schen Zahlen $2^{(2^n)} + 1$ für $n > 1$ der Menge M_{17} an.

Aus der Reihe (2) werden zwei Primzahlen herausgegriffen, die mit p und q bezeichnet werden. Es kann auch $p = q$ sein. Durch das Paar $(p\, q)$ wird eine Gruppe von Nichtprimzahlen festgelegt, die durch die Relation $p \cdot q \equiv c \bmod 30$ der Menge M_c angehört. Insgesamt sind $\binom{8}{2} + \binom{8}{1}$ Paarungen möglich, und damit 36 Gruppen von Nichtprimzahlen.

Auf die Zugehörigkeit einer Nichtprimzahl zu mindestens einer dieser Gruppen gründen sich die nachfolgend angegebenen Methoden zur Aufsuchung von Teilern einer Zahl Z.

Die Kenntnis aller Primzahlen $< \sqrt{Z}$ wird nicht vorausgesetzt. Dagegen lassen sich vorhandene Teiler aus arithmetischen Progressionen 1. und 2. Ordnung ablesen.

Auch ergeben sich spezielle Kriterien für Primzahlen und Primzahlzwillinge sowie Aussagen über die Teilungseigenschaften von Zahlenmannigfaltigkeiten.

Die höchste in Faktoren zerlegte Zahl ist in Beispiel (10) $Z_{11} = 2\,690\,801$.

In § 2 wird beispielsweise gezeigt:

Ist k eine Quadratzahl, so ist $30k + 11$ durch keine Primzahl der Reihe (2) – 11 ausgenommen – teilbar.

In Beispiel (15) werden eine Reihe von Primteilern aufgezeigt, durch die $30.2^n + 11$ nicht teilbar ist.

§ 1. Zerlegungsformen

1. Soll $Z = 30k + c$ ein Produkt von mindestens zwei ganzzahligen Faktoren sein, so muß die Form erscheinen

$$30k + c = (30x + p)(30y + q) \tag{3}$$

p und q sind zwei Primzahlen der Reihe (2), die durch die Kongruenz verbunden sind

$$p \cdot q \equiv c \bmod 30 \tag{4}$$

Setzt man also $p \cdot q = 30k_0 + c$, wobei k_0 als „Nullindex" bezeichnet wird, so erhält man

$$\begin{aligned} k &= 30\,xy + qx + py + k_0 \\ &= y(30x + p) + (qx + k_0) = x(30y + q) + (py + k_0). \end{aligned} \tag{5}$$

Ist Z_c nach (3) in Faktoren zerlegbar, so wird (pq) als Zeichen für die Zerlegungsform gebraucht. Vom Index k wird ausgesagt, er zerlege nach (pq).

In den Mengen M_7 M_{11} M_{13} M_{17} M_{23} M_{29} erscheinen je vier Zerlegungsformen. Sie sind zusammengestellt in

Tabelle I

	p	q	k_0		p	q	k_0
M_7	7	31	7	M_{17}	17	31	17
	17	11	6		7	11	2
	13	19	8		13	29	12
	23	29	22		23	19	14
M_{13}	7	19	4	M_{23}	7	29	6
	17	29	16		17	19	10
	13	31	13		13	11	4
	23	11	8		23	31	23
M_{11}	7	23	5	M_{29}	7	17	3
	17	13	7		13	23	9
	11	31	11		11	19	6
	19	29	18		31	29	29

In den Mengen M_{31} und M_{19}, in denen auch der Fall $p = q$ auftritt, erscheinen je sechs Zerlegungsformen.

Tabelle II

	7	13	2		11	29	10
	17	23	12		31	19	19
	11	11	3		7	7	1
M_{31}	19	19	11	M_{19}	17	17	9
	29	29	27		13	13	5
	31	31	31		23	23	17

Die folgenden Beispiele beschränken sich hauptsächlich auf die Menge M_{11}. Gelegentlich werden M_{13} und M_{17} herangezogen.

Ohne Beziehung zur Anordnung der Zahlen p und q in den Tabellen wird in den meisten Fällen $p < q$ gewählt.

Ein Index k zerlegt eine Z_{11}, wenn sich K nach Tabelle I in mindestens eine der vier Formen bringen läßt:

$$\begin{array}{ll} (11\ \ 31) & k = 30\,xy + 31\,x + 11\,y + 11 \\ (19\ \ 29) & k = 30\,xy + 29\,x + 19\,y + 18 \\ (\ 7\ \ 23) & k = 30\,xy + 23\,x + \ \ 7\,y + \ \ 5 \\ (13\ \ 17) & k = 30\,xy + 17\,x + 13\,y + \ \ 7 \end{array} \tag{6}$$

Nimmt k keine dieser vier Formen an, so ist $30\,k + 11$ Primzahl. Folgende Indizes zerlegen nach Tabelle I eine Z_{13}:

$$\begin{array}{ll} (\ 7\ \ 19) & k = 30\,xy + 19\,x + \ \ 7\,y + \ \ 4 \\ (17\ \ 29) & k = 30\,xy + 29\,x + 17\,y + 16 \\ (13\ \ 31) & k = 30\,xy + 31\,x + 13\,y + 13 \\ (23\ \ 11) & k = 30\,xy + 23\,x + 11\,y + \ \ 8 \end{array} \tag{7}$$

Ist ein Index k von allen in M_{11} und M_{13} vorkommenden Formen ausgeschlossen, so bringt er Primzahlzwillinge

$$30\,k + 11 \quad \text{und} \quad 30\,k + 13 \quad \text{hervor.}$$

2. Im folgenden wird die Gleichung (3) in der symbolischen Form geschrieben:

$$M_p \cdot M_q = M_c.$$

Ist $p = q$, so folgt aus Tabelle II, daß entweder

$$M_p \cdot M_p = M_{19} \text{ für } p = 7, 17, 13, 23 \qquad \text{Gruppe I}$$

oder (8)

$$M_p \cdot M_p = M_{31} \text{ für } p = 11, 31, 19, 29 \qquad \text{Gruppe II}$$

Erhebt man eine aus mindestens zwei Faktoren bestehende Zahl $30x + p$ der Gruppe I ins Quadrat, so ist nach Tabelle II das Quadrat des einen Faktors eine Zahl aus M_{31}, das des andern Faktors eine Zahl aus M_{19}. In jedem Fall erscheint also das Quadrat der Nichtprimzahl in der Zerlegungsform (31 19) und die Gleichung

$$(30x + p)^2 = (30u + 31)(30v + 19)$$

hat ganzzahlige Lösungen u und v.

Für den Index x gilt

$$30x^2 + 2px + \frac{p^2 - 19}{30} = 30uv + 19u + 31v + 19. \qquad (9)$$

Danach gilt der Satz:

$30x + p$ ist Primzahl für $p = 7, 17, 13, 23$, wenn die Gleichung (9) keine ganzzahligen Lösungen u und v besitzt.

3. Nach Tabelle I ist

$$M_{11} \cdot M_{13} = M_{23}.$$

Nimmt man in diesem Produkt mindestens einen Faktor als Nichtprimzahl an, so erscheint notwendig einer der beiden Faktoren M_{31} oder M_{19}.

Ist also mindestens eine der beiden Zahlen $30x + 11$, $30x + 13$ Nichtprimzahl, so erscheint das Produkt

$$(30x + 11)(30x + 13)$$

entweder in der Form $(30u + 31)(30v + 23)$ oder in der Form $(30u + 17)(30v + 19)$.

Für den Index x gilt: Mindestens eine der beiden Gleichungen

$$\begin{aligned} 30x^2 + 24x + 4 &= 30uv + 23u + 31v + 23 \\ 30x + 24x + 4 &= 30uv + 19u + 17v + 10 \end{aligned} \qquad (10)$$

hat ganzzahlige Lösungen.

Die Existenz beliebig hoher Primzahlzwillinge $30x+11$, $30x+13$ fällt demnach zusammen mit der Existenz beliebig hoher Zahlen x, für welche keine der beiden Gleichungen (10) durch ganze Zahlen lösbar ist.

4. Der Unterschied beider Gruppen kommt auch in den höheren Potenzen von M_c zum Ausdruck. Man findet aus den Tabellen:

Für die Gruppe I:

$$(M_7)^3 = M_{13} \quad (M_{13})^3 = M_7 \quad (M_{17})^3 = M_{23} \quad (M_{23})^3 = M_{17}. \quad (11)$$

In der Gruppe I gehört also die 9. Potenz von M_p wieder der M_p an.

Für die Gruppe II:

$$(M_{31})^n = M_{31} \quad (M_{11})^3 = M_{11} \quad (M_{19})^3 = M_{19} \quad (M_{29})^3 = M_{29}. \quad (12)$$

In der Gruppe II gehört die 3. Potenz von M_p wieder der M_p an. Speziell ist jede Potenz von M_{31} wieder eine M_{31}.

§ 2. Untersuchung einer Zahl auf ihre Zerlegbarkeit

1. $Z_c = 30k + c$ ist insbesondere durch q teilbar, wenn $y = 0$, $k = qx + k_0$; durch p teilbar, wenn $x = 0$, $k = py + k_0$.
Z_{11} ist teilbar durch

$$\begin{array}{llll} 11 \text{ wenn } k = 11y + 11 & \quad 31 \text{ wenn } k = 31x + 11 \\ 19 \text{ wenn } k = 19y + 18 & \quad 29 \text{ wenn } k = 29x + 18 \\ 7 \text{ wenn } k = 7y + 5 & \quad 23 \text{ wenn } k = 23x + 5 \\ 13 \text{ wenn } k = 13y + 7 & \quad 17 \text{ wenn } k = 17x + 7 \end{array} \quad (13)$$

Setzt man in den Gleichungen (6) $x = y = 1$, so erhält man als kleinsten Index in der Zerlegungsform (7 23) $k = 65$.
Die folgenden Indizes, da sie unter 65 liegen und in keiner der vorstehenden linearen Funktionen enthalten sind, führen auf Primzahlen P_{11}:

1, 2, 3, 4, 6, 8, 9, 10, 13, 14, 15, 16, 17, 21, 23, 25, 27, 29, 30, 31, 32, 34, 35, 36, 38, 39, 43, 45, 48, 49, 50, 52, 53, 57, 60, 62, 63, 64.

Hätte die Gleichung $w^2 = qx + k_0$ eine ganzzahlige Lösung $w = w_1$, so würden daraus zwei Reihen von Lösungen folgen:

$$w = w_1 + q\lambda \text{ und } w = q\lambda - w_1.$$

Ist die Gleichung demnach im Intervall

$$0 < w \leqq \frac{q-1}{2} \qquad 0 < x \leqq \frac{q-1}{2}$$

unlösbar, so ist sie für keinen Wert von x lösbar.
Auf diese Weise ergibt sich die Unlösbarkeit der Gleichungen

$$w^2 = qx + k_0 \quad \text{und} \quad w^2 = py + k_0$$

für die Menge M_{11}. Daher das Ergebnis:
$30w^2 + 11$ ist durch keine Primzahl der Reihe (2), 11 ausgenommen, teilbar.
Auf die gleiche Weise stellt man fest, daß $30\,w^3 + 11$ nicht durch 7 und 13 teilbar sein kann.

Nach (6) ist $30\,k + 11$ durch 37 teilbar, wenn $k = 37\,y + 28$. Man findet für $y = 8 : k = 324$, für $y = 9 : k = 361$.
Demnach ist $30\,w^2 + 11$ für $w = 18 + 37\,u$ und $w = 19 + 37\,u$ durch 37 teilbar.

2. Das Produkt

$$h = x \cdot y \qquad 30\,h = k - k_0 - qx - py. \tag{15}$$

Der Fall $h = 0$ ist in 1. vorweggenommen und werde im nachfolgenden ausgeschlossen.

Die Entscheidung, ob die Gleichung (5) bei gegebenem k lösbar ist, wird für relativ kleine Indizes dadurch sehr einfach, daß $h = x \cdot y$ kleiner als $(k - k_0) : 30$ sein muß.

Für h existiert übrigens eine irrationale obere Schranke h_m, die man erhält aus

$$x\,dy + y\,dx = 0 \qquad q\,dx + p\,dy = 0 \qquad x : y = p : q.$$

Man berechnet:

$$\begin{aligned} 30\sqrt{h_m} &= \sqrt{Z} - \sqrt{pq} \\ (k - k_0) : 30 - h_m &= (\sqrt{Zpq} - pq) : 900 \end{aligned} \tag{16}$$

Man erhält h_m auch durch Nullsetzen der Diskriminante der in x und in y quadratischen Gleichungen:

$$\begin{aligned} h(30x+p) &= x(k-k_0-qx) \\ h(30y+q) &= y(k-k_0-py). \end{aligned} \tag{17}$$

Man stellt fest:

Ist $k-k_0$ ungerade, so können x und y nicht beide ungerade sein. Dieser Fall schließt ungerade h aus.

Ist $k-k_0$ gerade, so sind x und y entweder beide gerade oder beide ungerade. Damit ist h entweder durch 4 teilbar oder es ist ungerade.

3. Zur Beantwortung der Frage, ob k nach (pq) zerlegt, genügt es für nicht zu große Indizes (5) nach y oder x aufzulösen:

$$y = \frac{k-(qx+k_0)}{30x+p} \qquad x = \frac{k-(py+k_0)}{30y+q}. \tag{18}$$

Für $x = 1, 2, 3, \ldots$ $y = 1, 2, 3, \ldots$ erscheinen die Brüche mit abnehmenden Zählern und zunehmenden Nennern.

Die Raschheit der Abnahme der Zähler kann gesteigert werden, wenn festgestellt ist, daß sich für $x \leqq a$ kein ganzzahliges y und für $y \leqq b$ kein ganzzahliges x einstellt. Man erhält die Brüche

$$\begin{aligned} x-a &= \frac{k-aq-k_0-y(30a+p)}{30y+q} \\ y-b &= \frac{k-bp-k_0-x(30b+q)}{30x+p}. \end{aligned} \tag{19}$$

Für die praktische Durchführung entwickelt man für die Zähler eine fallende, für die Nenner eine steigende arithmetische Progression. Wirkungsvoller und daher auf größere Zahlen anwendbar erweisen sich die in den §§ 3 und 4 dargelegten Methoden.

§ 3. Die Serienmethode

Ersetzt man in der Gleichung (5) x durch $x+n$ und y durch $y+n$, so geht sie über in

$$\begin{aligned} d &= (k - k_0) - (30n^2 + np + nq) \\ &= 30xy + x(30n + q) + y(30n + p). \end{aligned} \tag{20}$$

Setzt man der Reihe nach $n = 0, 1, 2, 3 \ldots$, so erhält man eine Serie von Gleichungen, die spätestens dann abbricht, wenn d die Koeffizienten der rechten Seite unterschreitet. Wird keine in der Serie enthaltene Gleichung durch $x = 0$ oder $y = 0$ erfüllt, so zerlegt k nicht nach (pq).

Ist Z zerlegbar, so findet sich in der Serie eine Gleichung, die für $y = 0$ eine ganzzahlige Lösung $x = x_0$ liefert, und eine andere Gleichung, die für $x = 0$ eine Lösung $y = y_0$ liefert. Beide Gleichungen können auch in eine Gleichung zusammenfallen. Bei der Durchführung der Methode kann vorteilhaft das Schema verwendet werden:

$$\begin{array}{lcc} d & \multicolumn{2}{c}{\text{Teiler}} \\ k - k_0 & p & q \\ k - k_0 - 30 - (p + q) & 30 + p & 30 + q \\ k - k_0 - 120 - 2\,(p + q) & 60 + p & 60 + q \\ k - k_0 - 270 - 3\,(p + q) & 90 + p & 90 + q \\ \ldots\ldots\ldots & \ldots & \ldots \end{array} \tag{21}$$

Für die Lösungen x_0 und y_0 zieht man aus dem Schema die Folgerungen:

1. Enthält d einen nur durch 2, 3 und 5 teilbaren Faktor, so enthält x_0 bzw. y_0 denselben Faktor, da $30n + p$ und $30n + q$ nicht durch 2, 3, 5 teilbar sind.

Für (7 23) und (13 17) ist $30n^2 + n(p + q)$ durch 60 teilbar. Ist speziellerweise auch $k - k_0$ durch 60 teilbar, so sind x_0 und y_0 ebenfalls durch 60 teilbar. Dieser Umstand erlaubt ein rasches Abbrechen der Serie.

2. Für (7 23) und (13 17) endigt d stets auf die gleiche Ziffer. Da auch $30n + p$ und $30n + q$ gleichbleibende Endziffern aufweisen, so sind die Endziffern von x_0 und y_0 bekannt.

Beispiel (1)

Für den Index $k = 1445$ ($Z_{11} = 43361$) und die Zerlegungsform (31 11) erscheint die Serie:

	1434	11	31	717
	1362	41	61	681
$43361 = 131 \cdot 331$	1230	71	91	615
	1038	101	121	519
	786	131	151	393

Beispiel (2)

Für den Index $k = 605$ ($Z_{11} = 18161$) und die Zerlegungsform (7 23) erscheint:

x_0 und y_0 durch 60	600	7	23
teilbar	540	37	53
	..	..	..

$k = 605$ zerlegt nicht nach (7 23).

Beispiel (3)

$Z_{11} = 41711 = 30.1392 + 11$

Schema für (7 23)	1387	7	23
	1327	37	53
y_0 endet auf 1	1207	67	83
x_0 endet auf 9	787	97	..
	..	..	

Schema für (13 17)	1385	13	17	277
	1325	43	47	265
x_0 und y_0 endigen auf 5	1205	73	77	241
	1025	103	107	205
	785	133	137	157
	..	..	..	

41711 ist weder nach (7 23) noch nach (13 17) zerlegbar.

§ 4. Die Parametermethode

Nach § 1, 3 wurde die Nichtprimzahl Z in der Form angenommen

$$Z = (30x + p)\ (30y + q).$$

Unter dieser Voraussetzung existiert nach (16) für h eine irrationale obere Schranke h_m.

Diese obere Schranke existiert nicht mehr, wenn man Z in die Form setzt:

$$Z = (30\,x + p)\,(30y - q), \tag{22}$$

wobei $\qquad -p \cdot q \equiv c \; mod\; 30.$

Der Nullindex ist dann zu definieren durch

$$30\,k_0 - c = p \cdot q. \tag{23}$$

I

Nach der Parametermethode nimmt man in M_{11} für die Zerlegungsformen (7 23) und (13 17) Z in der Form

$$\begin{aligned} Z &= (30x + p)\,(30y - p) && \text{für} \quad p = 7 : k_0 = 2 \\ k + k_0 &= 30xy + p\,(y - x) && \text{für} \quad p = 13 : k_0 = 6. \end{aligned} \tag{24}$$

Um den Index k näher zu charakterisieren, bestimmt man zwei Größen A und B so, daß

$$k + k_0 = 30\,A + p\,B. \tag{25}$$

Man kann A in $A - p\varrho$ und B in $B + 30\varrho$ transformieren und bemerkt, daß man ein ungerades B nicht in ein gerades und umgekehrt verwandeln kann.

Mit Einführung des Parameters z zerfällt (24) in

$$x \cdot y = A - pz \qquad y - x = B + 30z. \tag{26}$$

Damit wird

$$(B + 30z)^2 + 4\,(A - pz) = (x + y)^2 = s^2 \tag{27}$$

eine Quadratzahl. Daher das Ergebnis:

Z ist nach $(p\ -p)$ zerlegbar, wenn sich zwei Zahlen

$$B_0 = B + 30z \quad \text{und} \quad A_0 = A - pz$$

finden lassen, so daß $B_0^2 + 4A_0 = s^2$ wird.
Erfüllen die beiden Teiler $30x + p$ und $30y - p$ die Ungleichung

$$-30 < y - x - B < 30, \tag{28}$$

so wird die Zerlegung mit $z = 0$ geleistet.

Beispiel (4)

Es ist $Z_{11} = 77381$ $(k = 2579)$ auf die Zerlegbarkeit nach $(13\ \ 17)$ zu prüfen.

$$k + 6 = 2585 = 2520 + 65 \qquad A = 84\ B = 5$$

$$B^2 + 4A = 19^2 \qquad 77381 = 223 \cdot 347$$

Man unterscheidet die Fälle:

1. Ist B gerade, so muß im Fall der Zerlegbarkeit schon $\left(\frac{B}{2} + 15z\right)^2 + A - pz$ eine Quadratzahl werden.

2. B ist ungerade. Ist dann A gerade, so ist auch z gerade, und man ersetzt z durch $2z$.

Ist A ungerade, so ist auch z ungerade, und man ersetzt z durch $2z + 1$.

Zur Auffindung relativ kleiner Teiler für relativ große Z stellt man mit Hilfe von (26) z als Funktion von x und als Funktion von y dar:

$$z(30x + p) = A - Bx - x^2 \quad z(30y - p) = y^2 - By - A. \tag{29}$$

z ist als Funktion von x monoton fallend, als Funktion von y monoton steigend. Daraus ergeben sich für z eine untere Schranke z_1 und eine obere Schranke z_2, wenn bekannt ist, daß z für keine Zahl $x \leq a$ und für keine Zahl $y \leq b$ ganzzahlig wird.

z liegt dann im Intervall

$$z_1 < z < z_2$$

mit

$$z_1(30b - p) = b^2 - Bb - A \quad z_2(30a + p) = A - Ba - a^2. \tag{30}$$

Man berechnet

$$30(z_2 - z_1) = (a + b)\left[\frac{Z}{(30a + p)\,(30b - p)} - 1\right]. \qquad (31)$$

Danach ist die Intervallbreite von A und B unabhängig.

Für die praktische Anwendung entwickelt man aus den rechten Gleichungsseiten in (29) arithmetische Reihen 2. Ordnung.

Beispiel (5)

Es ist $Z_{11} = 2\ 081\ 321$ auf Teiler der Form $30x + 13$ zu untersuchen.

$$k + 6 = 69\ 383 = 30 \cdot 2308 + 13 \cdot 11$$

z ersetzt durch $2z$

$$z(30x + 13) = 1154 - \frac{11x + x^2}{2}$$

1154		:	13
	6		
1148		:	43
	7		
1141		:	73
	8		
1133		:	103

$x = 3 \quad z = 11 \quad y = 674$

$2\ 081\ 321 = 103 \cdot 20207$

Beispiel (6)

Es ist $Z_{11} = 1\ 126\ 841$ auf die Zerlegbarkeit nach (7 23) zu untersuchen.

$$k + 2 = 37563 = 30 \cdot 1250 + 7 \cdot 9 \qquad A = 1250 \qquad B = 9$$

z wird durch $2z$ ersetzt.

$$z(30x + 7) = 625 - \frac{9x + x^2}{2} \qquad z(30y - 7) = -625 + \frac{y^2 - 9y}{2}$$

625		:	7
	5		
620		:	37
	6		
614		:	67
	7		
607		:	97
	8		
599		:	127
	9		
590		:	157
	10		
580		:	187
	11		
569		:	217
	12		
557		:	247
	13		
544		:	277
	14		

−629		:	23
	3		
632		:	53
	2		
634		:	83
	1		
635		:	113
	0		
635		:	143
	−1		
634		:	173
	2		
632		:	203
	3		
629		:	233
	4		
625		:	263
	5		
620		:	293
	6		

Danach bleiben nur noch die Werte $z = 1, 0, -1$;

Für keinen dieser drei Werte wird nach (27)

$$(9 + 60z)^2 + 4(1250 - 14z)$$

eine Quadratzahl.

$$Z = 1\ 126\ 841$$

zerlegt nicht nach (7 23).

Zur Ausschaltung von Parameterwerten, die auf keine Zerlegung führen, bieten sich noch folgende Möglichkeiten:

1. Soll $(B + 30z)^2 + 4(A - pz)$ eine Quadratzahl sein, so muß

$$(B^2 + 4A) + z(60B - 4p)$$

auf eines der folgenden 22 Endziffernpaare endigen:

$$\begin{matrix} 00 & 01 & 21 & 41 & 61 & 81 & \quad 04 & 24 & 44 & 64 & 84 \\ 25 & 16 & 36 & 56 & 76 & 96 & \quad 09 & 29 & 49 & 69 & 89 \end{matrix} \tag{32}$$

2. Es sei z ein Wert, der in (26) $x \cdot y = A - p \cdot z$ die rechte Gleichungsseite zur Primzahl P macht.

Ist dann z eine Lösung, so ist notwendig entweder $x = 1$ oder $y = 1$. Ist umgekehrt festgestellt, daß weder $x = 1$ noch $y = 1$ auf eine Zerlegung führen, so scheiden alle Parameterwerte aus, die $A - pz$ zu einer Primzahl machen.

Ist $A - pz = P \cdot P'$, wo P und P' beliebige Primzahlen, so löst z, wenn entweder $x = P$ oder $y = P$ eine Zerlegung ergeben. Ist dagegen festgestellt, daß weder $x = P$ noch $y = P$ auf eine Zerlegung führen, so scheiden alle Werte z aus, für welche $A - pz = P \cdot P'$.

(29) und (30) lassen sich zusammenfassen zu

$$\begin{aligned} (x - a)(y + a) &= (A - Ba - a^2) - z(30a + p) \\ (x + b)(y - b) &= (b^2 - Bb - A) - z(30b - p). \end{aligned} \tag{33}$$

Wenn $x - a = P$ und $y + a = P$ keine Zerlegung hervorbringen, so scheiden alle Werte z aus, die in (33) die rechte Gleichungsseite in die Form $P \cdot P'$ bringen.

Die vorstehenden Ausführungen lassen erkennen, daß die Parametermethode die Koinzidenz eines ganzzahligen x mit einem ganzzahligen y durch die Koinzidenz eines ganzzahligen x bzw. y mit einem ganzzahligen Parameterwert ersetzt.

Das graphische Bild der Funktionen in (29) macht die Wirkung der Methode deutlich: In der Umgebung von $x = 0$ verläuft der Hyperbelast steil und beim Übergang von x zu $x + 1$ ist die Änderung von z groß, so daß eine größere Anzahl von ganzzahligen Parameterwerten ausgeschaltet wird. Mit zunehmendem x verläuft der Kurvenast immer flacher, so daß beim Übergang von z zu $z + 1$ eine größere Anzahl von ganzzahligen Werten x ausgeschaltet wird.

Man berechnet diejenigen Kurvenpunkte, für welche

$$dz = -dx \quad \text{bzw.} \quad dz = dy$$

aus (26)

$$x\,dy + y\,dx + p\,dz = 0 \qquad dy - dx - 30\,dz = 0$$

und erhält:

$$\begin{aligned} &\text{für} \quad dz = -dx : y = 29x + p; \quad 29(30x + p)^2 = Z \\ &\text{für} \quad dz = dy : x = 29y - p; \quad 29(30y - p)^2 = Z. \end{aligned} \tag{34}$$

Für die Praxis kann daher gesetzt werden

$$30x \sim \sqrt{k} \quad \text{bzw.} \quad 30y \sim \sqrt{k}.$$

In der Umgebung dieser Werte sind demnach die absoluten Beträge der infinitesimalen Änderungen von x und z bzw. von y und z annähernd gleich groß.

II

Für alle Zerlegungsformen, bei denen $p + q$ von 30 verschieden ist, kann man die Indexdifferenz auf die Form bringen

$$k - k_0 = 30\,A + q\,B + p\,C. \tag{35}$$

Wählt man zwei voneinander unabhängige Zahlentripel a, b, c, welche die Gleichung erfüllen

$$0 = 30a + qb + pc,$$

so läßt sich die Gleichung (5) des § 1 mit Hilfe zweier Parameter u und v in das Gleichungssystem überführen:

$$\begin{aligned} xy &= A + a_1 u + a_2 v \\ x &= B + b_1 u + b_2 v \\ y &= C + c_1 u + c_2 v. \end{aligned} \tag{36}$$

Das Verfahren zielt dahin, die anfänglich willkürlich gewählten Größen A, B und C zu korrigieren und eine mögliche Zerlegung auf relativ kleine Parameterwerte zurückzuführen.

Ist von vornherein $A = B \cdot C$, so ist die Zerlegung mit $x = B$, $y = C$ gefunden.

Die Zerlegungsformen (31 11) und (19 29) der M_{11} werden in der Form (1 11) und (— 1 — 11) verwendet:

$$\begin{aligned} Z &= (30x + 1)(30y + 11) \qquad & Z &= (30x - 1)(30y - 11) \\ k &= 30xy + 11x + y & k &= 30xy - 11x - y. \end{aligned} \tag{37}$$

Für beide Formen bietet sich das Gleichungssystem an

$$\begin{aligned} xy &= A - e(u + 2v) \\ x &= B + 3u + 5v \\ y &= C - 3u + 5v. \end{aligned} \tag{38}$$

Dabei gilt $e = +1$ für (1 11), $e = -1$ für (— 1 — 11).

Man berechnet

$$\begin{aligned} 30x + p - (30y + q) &= 30(B - C + 6u) + p - q \\ &= 30x + p - Z:(30x + p) = Z:(30y + q) - (30y + q). \end{aligned}$$

Ist daher festgestellt, daß das Gleichungssystem (38) durch keine Zahl $x \leqq a$ und durch keine Zahl $y \leqq b$ erfüllt wird, so ergeben sich für u eine obere und eine untere Schranke.

u liegt im Intervall $u_1 < u < u_2$ mit

$$\begin{aligned} 30(B - C + 6u_1) &= (30a + p) - Z:(30a + p) \\ 30(B - C + 6u_2) &= Z:(30b + q) - (30b + q). \end{aligned} \tag{39}$$

Die Intervallbreite berechnet sich zu (40)

$$180(u_2 - u_1) = (30a + 30b + p + q)\left[\frac{Z}{(30a + p)(30b + q)} - 1\right].$$

Ebenso berechnet man

$$\begin{aligned}(30x + p) + (30y + q) &= 30(B + C + 10v) + p + q\\ = 30x + p + Z:(30x + p) &= Z:(30y + q) + 30y + q\end{aligned} \tag{41}$$

$x + y = s$ erreicht ein Minimum s_m für $30x + p = 30y + q$. Dadurch erreicht v ein Minimum v_m:

$$30s_m = 2\sqrt{Z} - (p + q) = 30(B + C + 10\,v_m). \tag{42}$$

Nunmehr kann man die willkürlich gewählten Größen A, B, C dadurch korrigieren, daß man in 38) v durch $v + [v_m] + 1$ ersetzt. Das Minimum ist damit nach $v = 0$ verlegt.
Ferner ergeben sich eine linksseitige obere Schranke v_1 und eine rechtsseitige obere Schranke v_2 aus

$$\begin{aligned}30(B + C + 10v_1) + p + q &= 30a + p + Z:(30a + p)\\ 30(B + C + 10v_2) + p + q &= Z:(30b + q) + 30b + q.\end{aligned} \tag{43}$$

Dazu zwei Intervallbreiten:

$$\begin{aligned}300(v_1 - v_m) &= \left[\sqrt{\frac{Z}{30a + p}} - \sqrt{30a + p}\right]^2\\ 300(v_2 - v_m) &= \left[\sqrt{\frac{Z}{30b + q}} - \sqrt{30b + q}\right]^2.\end{aligned} \tag{44}$$

Zerlegt Z tatsächlich in die beiden Teiler $30x + p$ und $30y + q$, so wird nach (44)

$$300(v + 1 + [v_m] - v_m) = \left(\sqrt{30x + p} - \sqrt{30y + q}\right)^2. \tag{45}$$

Danach wird die Zerlegung durch das ganzzahlige $v = 0$ geleistet, wenn das Quadrat der Differenz der Wurzeln aus beiden Teilern 300 unterschreitet.

Dies illustriert das folgende Beispiel:

Beispiel (7)

$Z_{11} = 743\,471$ ist auf einen Teiler der Form $30x - 1$ zu untersuchen.

$$k = 24782 = 30 \cdot 827 - 11 \cdot 2 - 6;\ v_m = 4{,}98;$$

v ersetzt durch $v + 5$: $A = 837$, $B = 27$, $C = 31$.
In diesem Fall ist das Gleichungssystem bereits durch

$$x = B = 27 \quad y = C = 31 \text{ gelöst. } 743\,471 = 809 \cdot 919.$$

Die Parametermethode liefert die Zerlegung desto rascher, je weniger sich die beiden Teiler voneinander unterscheiden.

Zur Auffindung relativ kleiner Teiler stelle man mit Hilfe von (38) u und v als Funktionen von x und von y dar.

$$\begin{aligned} u(30x + e) &= -5A - 2eB + x(5C - 5B + 2e) + 5x^2 \\ u(30y + 11e) &= 5A + 2eC + y(5C - 5B - 2e) - 5y^2 \\ v(30x + e) &= 3A + eB - x(3B + 3C + e) + 3x^2 \\ v(30y + 11e) &= 3A - eC - y(3B + 3C - e) + 3y^2. \end{aligned} \tag{46}$$

Dazu treten die Gleichungen:

$$\begin{aligned} &\text{a)} \quad (u + 2v)(30x + e) = A - x(11B + C) + 11x^2 \\ &\text{b)} \quad (u + 2v)(30y + 11e) = 11A - y(11B + C) - y^2. \end{aligned} \tag{47}$$

Im folgenden Beispiel wird (47) a verwendet. Die rechte Gleichungsseite liefert eine arithmetische Progression 2. Ordnung, die auf die mögliche Zerlegung führt.

Beispiel (8)

$Z = 1\,287\,521$ ist auf die Zerlegbarkeit nach (1 11) zu prüfen. $k = 42917 = 30 \cdot 1430 + 11 \cdot 1 + 6$; $v_m = 6{,}8$; v ersetzt durch $v + 7$; korrigiert: $A = 1416$ $B = 36$ $C = 41$;

$$(u + 2v)(30x + 1) = 1416 - 437x + 11x^2.$$

Die rechte Gleichungsseite ist stets gerade. Daher ist u gerade und es genügt die Halbierung der Glieder der arithmetischen Progression.

495			: 31	$u + 2v = -6 \quad x \cdot y = 1422$
	202			
293		11	: 61	$y = 158$
	191			
102		11	: 91	
	180			
− 78			: 121	
	169			
− 247			: 151	$1\,287\,521 = 271 \cdot 4751$
	158			
405			: 181	
	147			
552			: 211	
	136			
688			: 241	
	125			
813			: 271	$x = 9.$

Nach (38) sind u und v durch die Relation verbunden:

$$A - e(u + 2v) = (B + 5v + 3u)(C + 5v - 3u) \tag{48}$$
$$9u^2 - u(3C - 3B + e) + A - BC = 25v^2 + v(5B + 5C + 2e).$$

Da $3C - 3B + e$ und $5B + 5C + 2e$ nicht gleichzeitig gerade oder ungerade sein können, so bemerkt man:

$$\begin{aligned}&\text{Ist } B + C\ (B - C) \text{ gerade, so ist } A - BC - 25v^2 \text{ gerade}\\ &\text{Ist } B + C\ (B - C) \text{ ungerade, so ist } A - BC + 9u^2 \text{ gerade.}\end{aligned} \tag{49}$$

Hieraus folgt die Übersicht:

$B + C$ gerade	$A - BC$ gerade	v ersetzt durch $2v$
	$A - BC$ ungerade	v ersetzt durch $2v + 1$
$B + C$ ungerade	$A - BC$ gerade	u ersetzt durch $2u$
	$A - BC$ ungerade	u ersetzt durch $2u + 1$.

Dieses Ergebnis hat eine Erweiterung von (45) zur Folge, derart, daß in weit mehr Fällen die Zerlegung durch $v = 0$ geleistet wird.

Beispiel (9)

$Z = 2\,451\,731$ ist auf die Zerlegbarkeit nach (—1 —11) zu untersuchen.

$$k = 81724 \quad A = 2725 \quad B = 2 \quad C = 4 \quad v_m = 10{,}75;$$

v ersetzt durch $v + 11$; korrigiert: $A = 2747 \quad B = 57 \quad C = 59$

$9u^2 - 5u - 616 = 25v^2 + 578v$; $v = 0$, $u = -8$, $x = 33$, $y = 83$

$$2\,451\,731 = 989 \cdot 2479.$$

Im allgemeinen Fall entwickelt man aus den beiden Gleichungsseiten von (48) arithmetische Progressionen 2. Ordnung, wobei v nur positiv, u sowohl positiv als negativ einzusetzen ist. Eine mögliche Zerlegung wird dadurch offenbar, daß in beiden Progressionen das gleiche Glied auftritt.

Diese Gegenüberstellung von zwei arithmetischen Progressionen erfordert für die Auffindung von Faktoren an Stelle von Divisionen nur Additionen und Subtraktionen.

Beispiel (10)

Es ist $Z = 2\,690\,801$ auf die Zerlegbarkeit nach $(-1\ -11)$ zu untersuchen.

$$k = 89693 = 30 \cdot 2990 - 0 \cdot 11 - 7 \cdot 1 \qquad v_m = 10{,}3.$$

Korrigiert:

$$A = 3012 \qquad B = 55 \qquad C = 62 \qquad A - BC = -398$$

u ersetzt durch $2u$;

$$18u^2 - 20u - 199 = \frac{25v^2 + 583v}{2}$$

$u = -3$	23			$v = 0$	0		
		146				304	
-4	169		36	1	304		25
		182				329	
-5	351		36	2	633		25
		218				354	
-6	569			3	987		
		254				379	
-7	823			4	1366		
		290				404	
-8	1113			5	1770		
		326				429	
-9	1439			6	2199		
		362					
-10	1801						
		398					
-11	2199						

$v = 6,\ u = -11,\ x = 19,\ y = 158;\ 2\,690\,801 = 569 \cdot 4729.$

§ 5. Zerspaltung von Zerlegungsformen

Nach § 1, 5 nimmt der Index k die Formen an

$$\begin{aligned} k &= y(30x + p) + qx + k_0 = y(30x + p) + a_1 \\ k &= x(30y + q) + pq + k_0 = x(30y + q) + a_2. \end{aligned} \tag{50}$$

a_1 wird als das „Adnexum" des Teilers $30x + p$ bezeichnet; $k = a_1$ ist der kleinste Index, der nach $30x + p$ zerlegt. Ebenso heiße a_2 das Adnexum des Teilers $30y + q$; a_2 ist der kleinste Index mit dem Teiler $30y + q$.

Die Aufspaltung der Zerlegungsform $(p\ q)$ in eine Reihe von untergeordneten Zerlegungsformen tritt ein beim Übergang vom Index k zum Index K durch die Gleichung

$$k = mK, \tag{51}$$

wo m eine beliebige ganze positive Zahl bedeutet.
Man setzt an Stelle von x

$$x + mu \quad x < m$$

und an Stelle von y

$$y + mv \quad y < m.$$

$$\begin{aligned} Z &= 30mK + c = (30mu + 30x + p)(30mv + 30y + q) \\ K &= 30muv + u(30y + q) + v(30x + p) + K_0, \end{aligned} \tag{52}$$

wobei $$K_0 = (30xy + qx + py + k_0) : m$$

$$30mK_0 + c = (30x + p)(30y + q). \tag{52a}$$

Die Beispiele werden auf drei einfache Fälle beschränkt:

1. m ist ein Teiler von 30:

Es ist die lineare diophantische Gleichung zu lösen

$$qx + py + k_0 \equiv 0 \bmod m.$$

Sie ordnet jedem Wert von x einen Wert von y zu und es erscheinen m Wertepaare.

Ist insbesondere $k = 2K$, so geht $k = y(30x + p) + a_1$ über in die Form

$$K = w(30x + p) + A_1,$$ wobei

$$A_1 = \frac{a_1}{2} \text{ für gerade } a_1, \quad A_1 = \frac{30x + p + a_1}{2} \text{ für ungerade } a_1. \tag{53}$$

A_1 heiße das Adnexum des Teilers $30x + p$ in bezug auf den Index K. Der Übergang von k zu $K = \frac{k}{2}$ werde als „Halbierung" bezeichnet.

2. Ist $m = 2^n$, so ist die Halbierung n mal zu wiederholen.

Beispiel (11)

Die nachfolgend herangezogenen Indizes treten nach Tabelle I in M_{11} auf. Bei fortgesetzter Halbierung von

$k = 7y + 5$ erscheinen die Adnexa $A = 6, 3, 5$;

$k = 17x + 7: A = 12, 6, 3, 10, 5, 11, 14, 7$;

$k = 23x + 5: A = 14, 7, 15, 19, 21, 22, 11, 17, 20, 10, 5$;

$k = 31y + 11: A = 21, 26, 13, 22, 11$;

$k = 127y + 97: A = 112, 56, 28, 14, 7, 67, 97$;

$k = 257x + 111: A = 184, 92, 46, 23, 140, 70, 35, 146, 73, 165, 211, 234, 117, 187, 222, 111$;

In allen Fällen fehlen Adnexa der Form 2^n.

Hieraus ist zu schließen:

$Z_{11} = 30 \cdot 2^n + 11$ ist nicht durch 7, 17, 23, 31, 127, 257 teilbar.

Beispiel (12)

Nach § 1 gehören die Gaußschen Zahlen der Menge M_{17} an. Nach Tabelle I treten in M_{17} die Zerlegungsformen auf:

$$(11\ 7) \quad (31\ 17) \quad (29\ 13) \quad (19\ 23).$$

Aus $2^{(2^n)} + 1 = 30k + 17$ folgt unmittelbar, daß für $n \geqq 2$ k durch 8 teilbar sein muß. Die Gaußschen Zahlen erscheinen demnach in der Form

$$G = 240K + 17.$$

Jede der obigen vier Zerlegungsformen zerfällt danach in 8 untergeordnete Zerlegungsformen, so daß sich für G als Nichtprimzahl 32 Zerlegungsformen einstellen.

Die aus (11 7) hervorgehenden Formen lassen sich wie folgt entwickeln:

$$k = 30xy + 11x + 7y + 2 = 8K.$$

Es genügt, $-2xy + 3x - y + 2$ zu einem Multiplum von 8 zu machen. Man gelangt stufenweise zu dem Ergebnis:

$$x - y = 2m;\ m = 2n - 1; \qquad n = -2u + \frac{x + x^2}{2}$$
$$y = 2 - x - 2x^2 + 8u \qquad x = 2 - y - 2y^2 + 8v. \tag{54}$$

Die beiden Gleichungen (54) sind äquivalent insofern, als sie die gleichen Wertepaare x, y liefern:

x	0	1	2	3	4	5	6	7	Teiler	$30x + 7$
y	2	7	0	5	6	3	4	1		$30y + 11$

Die Form (11 7) zerfällt demnach in die 8 Unterformen

(7 71) (37 221) (67 11) (97 161)

(127 191) (157 101) (187 131) (217 41).

Für die Gaußschen Zahlen besteht die Rekursionsformel

$$G_{n+1} - 1 = (G_n - 1)^2.$$

Hieraus geht für die Indizes die Rekursionsformel hervor

$$K_{n+1} = 240K_n^2 + 32K_n + 1. \tag{55}$$

3. Es sei m eine Primzahl $m = P > 5$ und verschieden von c. Dann scheiden in 52) alle Werte $x = x_0$ aus, für welche $30x_0 + p$ durch P teilbar ist, und ebenso alle Werte $y = y_0$, für welche $30y_0 + q$ durch P teilbar ist.
Es sei

$$30x_0 + p = P\lambda \quad 30y_0 + q = P\mu. \tag{56}$$

Dann läßt sich (52) a) in der Form schreiben

$$30PK_0 + c = [30(x - x_0) + P\lambda]\,[30(y - y_0) + P\mu]$$

und es erscheint für x und y die Bedingung

$$900(x - x_0)\,(y - y_0) \equiv c \bmod P \tag{57}$$

für alle möglichen Zerlegungsformen der M_c.
Es erscheinen $P - 1$ Lösungspaare x, y.

Ersetzt man in der Reihe (2) des § 1 die Zahl 31 durch 1, so lassen sich die Primzahlen der Reihe viermal paarweise zur Summe 30 zusammenfassen. Es seien p_1 und p_2 zwei solche

Primzahlen mit der Summe 30, und $30x_0 + p_1$ sowie $30y_0 + p_2$ seien durch P teilbar.

Dann gilt

$$30x_0 + p_1 + 30y_0 + p_2 = P(\lambda + \mu).$$

Demnach ist $\lambda + \mu$ ein Multiplum von 30. Setzt man fest, daß es 30 nicht übersteigen soll, so wird

$$x_0 + y_0 + 1 = P. \tag{58}$$

Das folgende Beispiel bezieht sich auf die Menge M_{11} und auf die Primzahl $P = 13$.

Beispiel (13)

nach (57): $\qquad 900(x - x_0)(y - y_0) \equiv 11 \bmod 13$

$$(x - x_0)(y - y_0) \equiv 8 \bmod 13$$

$(x - x_0)$	1	2	3	4	5	6	7	8	9	10	11	12
$(y - y_0)$	8	4	7	2	12	10	3	1	11	6	9	5

Die Wertpaare x, y für die vier Zerlegungsformen sowie die zugehörigen Werte K_0 zeigt

Tabelle III

(1 11)			(7 23)			(13 17)			(19 29)		
x	y	K_0	x	y	K_0	x	y	K_0	x	y	K_0
0	0	0	0	3	2	0	–	–	0	10	16
1	3	8	1	1	5	1	7	25	1	7	30
2	12	58	2	7	40	2	3	20	2	2	18
3	–	–	3	5	43	3	6	52	3	5	50
4	2	22	4	2	27	4	1	6	4	1	21
5	11	132	5	10	130	5	11	145	5	–	–
6	1	19	6	0	11	6	9	142	6	4	76
7	9	152	7	9	163	7	2	44	7	0	17
8	6	118	8	–	–	8	0	11	8	3	79
9	4	91	9	12	272	9	10	230	9	11	266
10	10	240	10	8	207	10	5	134	10	8	220
11	8	213	11	11	305	11	8	226	11	6	187
12	5	149	12	6	191	12	4	131	12	12	378
–	7	–	–	4	–	–	12	–	–	9	–

Die Tabelle enthält auch alle Werte x_0, y_0 für jede Form.

Trägt man für die Zerlegungsformen (7 23) und (13 17) die Wertpaare x, y aus der Tabelle III in die Gitterpunkte eines rechtwinkeligen Koordinatensystems ein, so liegen auf Grund der Relation (58) für jede Form die besetzten Gitterpunkte symmetrisch zur Geraden $x + y + 1 = 13$.

Zur selben Geraden symmetrisch ordnen sich die besetzten Gitterpunkte, wenn man die Wertepaare x, y gleichzeitig für die Formen (1 11) und (19 29) einträgt. Es sei

x_m = arithm. Mittel aus den 4 Werten $x_0 = (0 + 3 + 5 + 8) : 4$

y_m = arithm. Mittel aus den 4 Werten $y_0 = (7 + 4 + 12 + 9) : 4$

$$x_m = 4 \qquad y_m = 8.$$

Man trägt die Wertepaare $x + 13u$ und $y + 13v$ für alle vier Zerlegungsformen in das Koordinatensystem ein und teilt die Bildebene in quadratische Bereiche mit der Berandung

$$\begin{array}{ll} x_m + 13u & x_m + 13u + 13 \\ y_m + 13v & y_m + 13v + 13. \end{array}$$

In jedem solchen Bereich wiederholt sich eine zur Geraden

$$x + y - 12 = 13(u + v + 1)$$

und zur Geraden

$$x - y + 4 = 13(u - v)$$

symmetrische Punktanordnung, die eine bemerkenswerte Regelmäßigkeit zeigt.

Insbesondere enthält der quadratische Bereich 12 doppelt besetzte Gitterpunkte, die auf einem Kreis liegen, dessen Mittelpunkt in den Mittelpunkt des Bereiches fällt. Sein Radius ist

$$\frac{1}{2}\sqrt{13^2 + 1}.$$

Ordnet man die Werte K_0 nach der Größe: $K_0 = 1, 4, 6, 8, \ldots$, so liest man die Primzahlindizes ab: $K = 2, 3, 5, 7, 9, 10, \ldots$.

Es sei allgemein m eine beliebige Zahl und der den Teiler 7 hervorbringende Index $K \equiv A \bmod 7$ $(A < 7)$.

Ferner sei ε die kleinere der beiden Zahlen 11 und $7 + A$.

Fallen dann in das Intervall 0 bis $\varepsilon\, n$ Werte K_0, so liegen im gleichen Intervall $\varepsilon - n$ Primzahlindizes.

Im allgemeinen füllen die Werte K_0 das Intervall von 0 bis ε nicht lückenlos aus. Es ist jedoch evident, daß man Zahlen m konstruieren kann, die vorgegebenen Teilern vorgeschriebene Werte K_0 zuordnen.

Beispiel (14)

$30 m K_0 + 11$ soll teilbar sein: für $K_0 = 1$ durch 7
für $K_0 = 2$ durch 13
für $K_0 = 3$ durch 17.

Es sind die Kongruenzen zu lösen:

$$1 \cdot m \equiv 5 \bmod 7 \quad 2 \cdot m \equiv 7 \bmod 13 \quad 3 \cdot m \equiv 7 \bmod 17.$$

Man findet als kleinste Zahl $m = 348$.
Demnach ist nach Vorschrift $30 \cdot 348\, K + 11$ für $K = 1, 2, 3$ Nichtprimzahl.

Für $K = 4$ erscheint die Zahl $Z = 41711$. Man weist sie mit Hilfe der Methoden in § 3 und 4 als Primzahl nach.