ZAHLEN DER FORM $x^2 - Dy^2$ IN ARITHMETISCHEN FOLGEN (*)

von KLAUS SPINDELBÖCK (in Graz) (**)

SOMMARIO. - *In questo lavoro si esamina la questione se in una successione aritmetica* $(at + b/t = 0, 1, 2, ...)$ *possono comparire numeri della forma* $x^2 - Dy^2$ $(x, y, D \in Z)$.

SUMMARY. - *In this paper we investigate if in any arithmetic succession* $(at + b/t = 0, 1, 2, ...)$ *may appear numbers of the type* $x^2 - Dy^2$ $(x, y, D \in Z)$.

In [1] teilt P. Bronkhorst mit, dass in jeder arithmetischen Folge, deren Differenz eine Primzahl ist, unendlich viele Zahlen auftreten, die sich als Summe zweier Quadrate darstellen lassen.

Hier soll die Frage untersucht werden, ob in einer arithmetischen Folge $(at+b/t=0, 1, 2, ...)$ Zahlen auftreten können, die die Form x^2-Dy^2 $(x, y, D \in \mathbb{Z})$ haben.

Zu bemerken ist, dass die Existenz einer einzigen Zahl dieser Art das Vorhandensein unendlich vieler Zahlen dieser Art in der arithmetischen Folge gewährleistet; denn gilt $at_0+b=x_0^2-Dy_0^2$, so ist $(x_0+ma)^2-D\,(y_0+na)^2$ eine Zahl der arithmetischen Folge.

Zunächst möchte ich noch einige Sätze erwähnen, auf die ich mich später beziehen werde:

HILFSSATZ: Zu jeder Primzahl $p>3$ gibt es eine Zahl $n \in \mathbb{N}$ derart, dass n quadratischer Rest und $n-1$ quadratischer Nichtrest mod p ist.

(*) Pervenuto in Redazione il 7 luglio 1974.

(**) Indirizzo dell'Autore: I. Mathematisches Institut - Universität Graz - Halbärthgasse 1 - A 8010 Graz (Austria).

ANMERKUNG: Theoretisch könnte der Fall eintreten, dass die ersten $(p-1)/2$ Werte im Restklassensystem (bei natürlicher Anordnung) nur quadratische Reste sind, die verbleibenden Werte quadratische Nichtreste.

BEWEIS: Hat p die Form $4k+1$, so kann der oben zitierte Fall nicht eintreten, weil -1 quadratischer Rest ist.

Ist p von der Form $4k+3$, so werden zwei Fälle unterschieden:

a) $p=8k+3$: Hier ist 2 quadr, Nichtrest, also tritt schon in der ersten Hälfte des Restsystems ein Nichtrest auf.

b) $p = 8k + 7$: 2 ist hier quadr. Rest, -1 quadr. Nichtrest. Mit $(p-1)/2 \equiv (-1)/2\,(p)$ erhält man, dass $(p-1)/2$ ein quadr. Nichtrest ist.

$(p-1)/2$ ist aber die letzte Zahl der ersten Hälfte und damit gibt es auch in der zweiten Hälfte einen quadr. Rest, z. B. $(p+1)/2$.

q. e. d.

SATZ 1: Eine Kongruenz

$$x^2 \equiv a\,(p^\alpha),\ (a,p)=1,\ \alpha>0,$$

p ungerade, hat entweder zwei Lösungen oder keine, je nachdem, ob a quadratischer Rest oder Nichtrest mod p ist.

SATZ 1*a*: Eine Kongruenz

$$x^2 \equiv a\,(2^\alpha),\ (a,2)=1$$

ist nur dann lösbar, falls $a\equiv 1\,(4)$ für $\alpha=2$ und $a\equiv 1\,(8)$ für $\alpha\geq 3$ ist. Sind diese Bedingungen erfüllt, so gibt es für $\alpha=1$ eine Lösung, für $\alpha=2$ zwei und für $\alpha\geq 3$ vier Lösungen.

SATZ 2: Für Kongruenzen der allgemeinen Form

$$x^2 \equiv a\,(m),\ m=2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}\ (a,m)=1$$

sind

$$a\equiv 1\,(4) \text{ für } \alpha=2,\ a\equiv 1\,(8) \text{ für } \alpha\geq 3,$$

$$\left(\frac{a}{p_1}\right)=1, \dots, \left(\frac{a}{p_k}\right)=1$$

notwendige Bedingungen für die Lösbarkeit.

Sind alle diese Bedingungen erfüllt, so ist die Anzahl der Lösungen gleich 2^k für $\alpha=0$ und $\alpha=1$, gleich 2^{k+1} für $\alpha=2$ und gleich 2^{k+2} für $\alpha\geq 3$.

BEWEIS: Siehe z. B. [2].

Im folgenden sollen drei Fälle einer arithmetischen Progression $an+b$ betrachtet werden:

I) $a=p$, p ungerade Primzahl

II) $a\equiv 1\ (2)$

III) $a=2^\alpha\ (\alpha\geq 2)$

1) $a=p$, p ungerade Primzahl.

SATZ 3: In jeder arithmetischen Folge $pn+b$ mit einer ungeraden Primzahl als Differenz gibt es unendlich viele Zahlen der Form x^2-Dy^2, falls $(D, p)=1$ ist.

Zum BEWEIS dieser Behauptung werden zwei Fälle unterschieden:

A) $-\frac{b}{D}$ quadr. Rest mod p B) $-\frac{b}{D}$ quadr. Nichtrest

Der Fall A) kann sehr schnell erledigt werden.

$-\frac{b}{D}\equiv y^2\ (p)$, und daraus ergeben sich die Kongruenzen

$$b\equiv -Dy^2\ (p) \text{ und } (pv)^2-Dy^2\equiv b\ (p).$$

Der Fall B) wird folgendermassen bewiesen:

1) $p=3$

Da $(-b)/D$ quadratischer Nichtrest mod 3 ist, ergibt sich $b/D\equiv 1$, also $b\equiv D\ (3)$.

Soll eine Darstellung $b\equiv x^2-Dy^2\ (3)$ existieren, so muss wegen $(D, 3)=1$ $x^2\equiv 1\ (3)$ gelten.

Ist $D\equiv 1\ (3)$ und $y\equiv 0\ (3)$, so gibt es die gesuchte Form, ebenso wie im Falle $D\equiv 2\ (3)$ und $y^2\equiv 1\ (3)$.

2) $p>3$

Hier sind zwei Unterfälle zu untersuchen

i) $$\left(\frac{b}{p}\right)=1, \quad \left(-\frac{D}{p}\right)=-1$$

ii) $$\left(\frac{b}{p}\right)=-1, \quad \left(-\frac{D}{p}\right)=1.$$

Für den Fall i) gibt es nach dem Hlifssatz unter den zu p primen Restklassen eine Zahl n mit $\left(\frac{n}{p}\right)=1$, sodass $\left(\frac{n-1}{p}\right)=-1$ ist. Damit erhält man

$$-\frac{b}{D}(n-1)\equiv v^2\,(p) \text{ und weiters } b\equiv bn+Dv^2\,(p).$$

Ist dabei $p=4k+1$, so ist $\left(\frac{-1}{p}\right)=1$ und deshalb ist auch $-v^2$ ein quadratischer Rest; auf diese Weise erhält man die gewünschte Darstellung.

Hat die Primzahl p die Form $4k+3$, so ist -1 quadratischer Nichtrest und damit D quadr, Rest; ausserdem gilt mit $\left(\frac{-b/D}{p}\right)=-1$ auch $\left(\frac{-bD}{p}\right)=-1$.

Mit obigem n folgt dann $\frac{-bD}{n-1}\equiv v^2\,(p)$, woraus man durch Umformen zur Kongruenz

$$b\equiv(-1/D)\cdot v^2\cdot n+v^2/D\,(p)$$

gelangt.

Da D ein quadr. Rest ist, gibt es dazu eine Quadratwurzel. Beachtet man dies, so folgt aus

$$b\equiv-\frac{D^2}{D}\cdot\frac{v^2n}{DD}+\left(\frac{v}{\sqrt{D}}\right)^2(p)$$

die Form $b\equiv x^2-Dy^2$.

Im Falle ii) ist $\left(\frac{b}{p}\right)=-1$ und damit $\left(\frac{-D}{p}\right)=1$.

Mit der Zahl n des Hilfssatzes ergibt sich für $p=4k+1$ die Kongruenz $\frac{b}{n-1}\equiv v^2\,(p)$ und damit $b\equiv nv^2-v^2\,(p)$; wegen $\left(\frac{-1}{p}\right)=1$ ist mit $-D$ auch D quadratischer Rest.

Setzt man $x\equiv\sqrt{n}\cdot v$, $y\equiv v/\sqrt{D}\,(p)$, so erhält man die gesuchte Form.

Hat p die Gestalt $4k+3$, so suche man unter den zu p primen Restklassen eine Zahl N heraus, für die gilt:

$$\left(\frac{-N}{p}\right)=1,\quad\left(\frac{-N+1}{p}\right)=-1.$$

Es folgt somit

$$\frac{-b}{D}(-N+1) \equiv v^2 \text{ und daraus } b \equiv bN - Dv^2 \,(p).$$

bN ist quadr. Rest, weil b und N quadr. Nichtreste sind.

q. e. d.

II) $a \equiv 1\,(2)$.

Später wird folgender HILFSSATZ verwendet:

Hat b nach zwei teilerfremden Moduln m_1 und m_2 eine Darstellung der Art

$$b \equiv x_i^2 - Dy_i^2 \,(m_i) \quad (i=1,2),$$

so kann b auch nach dem Produkt $m_1 \cdot m_2$ auf eine solche Form gebracht werden.

BEWEIS: Nach Voraussetzung gilt $b \equiv x_i^2 - Dy_i^2 \,(m_i)$, $(i=1,2)$. Mit Hilfe des Chinesischen Restsatzes ergibt sich:

$$(x) \qquad b \equiv \frac{m_2 x_1^2 + m_1 x_2^2}{m_1 + m_2} - D\,\frac{m_2 y_1^2 + m_1 y_2^2}{m_1 + m_2} \,(m_1 \cdot m_2).$$

Durch Ausrechnen verifiziert man die Kongruenz

$$\left(\frac{m_2 x_1 + m_1 x_2}{m_1 + m_2}\right)^2 \equiv \frac{m_2 x_1^2 + m_1 x_2^2}{m_1 + m_2} \,(m_1 \cdot m_2).$$

Eine analoge Kongruenz erhält man für den Faktor, der bei D steht. Setzt man dies in die Kongruenz (x) ein, so liefert dies tatsächlich eine Darstellung $b \equiv x^2 - Dy^2 \,(m_1 m_2)$.

Der Fall, in dem a eine Primzahl ist, wurde in I) behandelt.

Die kanonische Zerlegung von a laute: $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

1. FALL: Gilt für alle diese p_i, dass $(D, p_i)=1$ und $\left(\frac{-b/D}{p_i}\right) = 1$ ist, so ist auch $\left(\frac{-b/D}{a}\right) = 1$ und sogar $-b/D$ quadr. Rest mod a.

Setzt man z. B. $-b/D \equiv y^2\,(a)$, so folgt daraus $b \equiv -Dy^2\,(a)$ und damit $b \equiv (av)^2 - Dy^2\,(a)$.

2. FALL: $-b/D$ sei nicht nach allen Primteilern des Moduls a quadratischer Rest.

Da nach Satz 1 jede Zahl, die nach der ungeraden Primzahl p quadratischer Rest ist, auch nach allen höheren Potenzen von p quadratischer Rest ist und umgekehrt, können die im Fall B dargelegten Vorgangsweisen auch nach jeder höheren Primzahlpotenz angewendet werden.

Nach jeder Primzahlpotenz $p_i^{\alpha_i}$, die in a aufgeht, kann man nach Satz 3 für b eine Darstellung der Art

$$b \equiv x_i^2 - Dy_i^2 \ (p_i^{\alpha_i})$$

finden.

Zufolge des Hilfssatzes kommt man dann zur Darstellung

$$b \equiv x^2 - Dy^2 \ (a).$$

III) $a = 2^\alpha$.

Hier werde vorausgesetzt, dass sowohl b als auch D ungerade seien.

Da nach Voraussetzung b und D beide ungerade sein sollen, ergeben sich, um überhaupt die Darstellung $b \equiv x^2 - Dy^2 \mod 2^\alpha$ erhalten zu können, die notwendigen Bedingungen, dass $b \equiv 1\ (4)$ oder $-b/D \equiv 1\ (4)$ oder beides gilt.

1. Fall: $b \equiv 1\ (4)$

i) Ist $\alpha = 2$, so ist b quadr. Rest mod 4, die Darstellung $b \equiv x^2 - Dy^2\ (4)$ also möglich, wenn $x \equiv 1\ (2)$ und $y \equiv 0\ (2)$ sind.

$\alpha = 3$

a) $b \equiv 1\ (2^3)$. Hier ist b quadr. Rest mod 2^α $(\alpha \geq 3)$, die Darstellung also möglich.

b) $b \equiv 5\ (2^3)$. Wählt man $x \equiv 1\ (2)$, $y \equiv 2\ (4)$, so erhält man mod 8 unabhängig von D die gesuchte Darstellung.

ANMERKUNG: Mit $y^2 \equiv 4\ (8)$ gilt gleichzeitig $y^2 \equiv 4\ (32)$; da sich jede Zahl, die $\equiv 4\ (32)$ ist, als $4(8k+1)$ darstellen lässt, ist sie auch nach jeder höheren Potenz von 2 quadratischer Rest.

Nun soll gezeigt werden, dass im Fall $b \equiv 5\ (8)$ auch für $\alpha > 3$ die Darstellung $b \equiv x^2 - Dy^2\ (2^\alpha)$ möglich ist.

Dazu wird, ausgehend von der Darstellung für 2^3, die Darstellung für 2^α konstruiert.

Es gelte $b \equiv A - DB\ (8)$ mit $b \equiv 5\ (8)$, $D \equiv 1\ (2)$, $A \equiv 1\ (8)$, $B \equiv 4\ (2^5)$. Gesucht ist die Darstellung $b \equiv A - D \cdot B\ (2^\alpha)$.

ANSATZ:

$$b \equiv 5 + 2^3 K_1\ (2^\alpha),\quad D \equiv 1 + 2 K_2\ (2^{\alpha-2})$$

$$A \equiv 1 + 2^3 K_3\ (2^\alpha),\quad B \equiv 4 + 2^5 K_4\ (2^\alpha).$$

Daraus ergibt sich folgendes:

$$D \cdot B \equiv (2^{\alpha-2} j + 1 + 2 K_2)\ (4 + 2^5 K_4) \equiv 4 + 2^3 K_2 + 2^5 K_4 + 2^6 K_2 K_4\ (2^\alpha),$$

weiters

$$b + D \cdot B \equiv 1 + 2^3\ (1 + K_1 + K_2 + 2^2 K_4 + 2^3 K_2 K_4)\ (2^\alpha).$$

Wählt man demnach $K_3 \equiv 1 + K_1 + K_2 + 2^2 K_4 + 2^3 K_2 K_4\ (2^{\alpha-3})$, so ist die gewünschte Darstellung erreicht.

2. Fall: $\dfrac{-b}{D} \equiv 1\ (4)$.

1) $\alpha = 2$: $-b/D$ ist in diesem Fall quadr. Rest mod 4, woraus die Möglichkeit der Darstellung folgt.

ii) $\alpha = 3$

a) $-b/D \equiv 1\ (8)$. $-b/D$ ist hier quadr. Rest mod 2^α $(\alpha \geq 3)$, weshalb $b \equiv x^2 - Dy^2\ (2^\alpha)$ möglich ist.

b) $-b/D \equiv 5\ (8)$.

Wählt man $x \equiv 2\ (4)$, $y \equiv 1\ (2)$, so kann mod 8 die gesuchte Darstellung erreicht werden.

Auch in diesem Fall wird für $\alpha > 3$ eine Darstellung $b \equiv A - D \cdot B (2^\alpha)$ konstruiert, wobei man, ausgehend von einer Darstellung mod 8, berücksichtigen muss, dass $A \equiv 4\ (2^5)$ und $B \equiv 1\ (8)$ gilt.

Aus $-b/D \equiv 5 + 2^3 k\ (2^\alpha)$ ergibt sich $b/D \equiv 3 + 2^3 K_1\ (2^\alpha)$, also $b \equiv (3 + 2^3 K_1) \cdot D\ (2^\alpha)$.

Weiters gelte

$$A \equiv 4 + 2^5 K_4\ (2^\alpha)$$

$$B \equiv 1 + 2^3 K_3\ (2^\alpha)$$

$$D \equiv 1 + 2 K_2\ (2^{\alpha-2}).$$

Damit erhält man für $b+D\cdot B$:

$$b+D\cdot B\equiv D\,(2^2+2^3\,(K_1+K_3))\;(2^\alpha)$$

und weiters

$$b+D\cdot B\equiv\;(2^{\alpha-2}\,j+2\,K_2+1)\;(2^2+2^3\,(K_1+K_3))\equiv$$

$$\equiv 2^2+2^3\,(K_1+K_2+K_3)+2^4\,K_2\,(K_1+K_3)\;(2^\alpha).$$

Soll nun $b+D\cdot B\equiv A\;(2^\alpha)$ sein, so muss zwischen den $K_i\,(i=1,2,3,4)$ die Beziehung bestehen

$$K_1+K_2+2\,K_1\,K_2+K_3\,(1+2\,K_2)\equiv 2^2\,K_4\;\;(2^{\alpha-3}).$$

Da K_1 und K_2 durch Vorgabe der Werte von b und D bekannt sind, ist diese Kongruenz eigentlich nur eine Beziehung zwischen K_3 und K_4. Sie ist nicht für beliebige Werte von K_3 und K_4 erfüllt, doch ist dies auch nicht nötig, weil nur die Existenz einer einzigen derartigen Kombination erforderlich ist.

Aufgrund der Definitionen der $K_i\,(i=3,4)$ muss K_4 weniger Werte durchlaufen als K_3, denn es gelten die Bedingungen $0\leq K_4\leq 2^{\alpha-5}-1$ und $0\leq K_3\leq 2^{\alpha-3}-1$; deshalb ist es vorteilhaft, K_4 vorzugeben und hierauf das zugeordnete K_3 zu bestimmen.

Dann gilt

$$K_3\equiv\frac{4K_4-2K_1\,K_2-(K_1+K_2)}{1+2K_2}\;(2^{\alpha-3}).$$

q. e. d.

ANMERKUNG: Im Falle $a=2$ existiert für beliebige Werte von b und D stets eine Darstellung $b\equiv x^2-Dy^2\;(2)$.

ANMERKUNG: Hat a die Gestalt $a=2^\alpha\cdot p$ beziehungsweise $a=2^\alpha\,p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, so sind entsprechend dem Hilfssatz unter II die geeigneten Fälle zu kombinieren.

Ergänzungen:

Bisher wurde bei der Darstellung $b\equiv x^2-Dy^2$ nur der Fall zugelassen, dass sowohl b als auch D ungerade waren, wenn der Modul 2^α war.

Nun sollen für solche Moduln auch die anderen möglichen Kombinationen für b und D untersucht werden und wenn möglich, auch die entsprechenden Bedingungen aufgestellt werden. Dazu sind drei Fälle zu unterscheiden:

I. b gerade, D ungerade

II. b ungerade, D gerade

III. b gerade, D gerade.

ANMERKUNG: Beim Aufstellen der Bedingungen wird so vorgegangen, dass man sich b, D, y^2 vorgegeben denkt, und hierauf das zugehörige x^2 bestimmt.

I. Fall:

b gerade, D ungerade

modulo 8 ergeben sich die folgenden Kombinationen:

x	y	b	D
0 (4)	0 (4)	0 (8)	1 (2)
0 (4)	2 (4)	4 (8)	1 (2)
2 (4)	0 (4)	4 (8)	1 (2)
2 (4)	2 (4)	0 (8)	1 (2)
1 (2)	1 (2)	0 (8)	1 (8)
		−2 (8)	3 (8)
		4 (8)	−3 (8)
		2 (8)	−1 (8)

a) $x \equiv 2\ (4),\ y \equiv 2\ (4)$

$b \equiv 2^3 K_1,\ D \equiv 1 + 2 K_2,\ x^2 \equiv 4 + 2^5 K_3,$

$y^2 \equiv 4 + 2^5 K_4$ mit $K_1 + K_2 \equiv 0\ (4)$.

Dann gilt für K_3:

$$K_3 \equiv 1/4 \cdot (K_1 + K_2) + K_4 + 2 K_2 K_4\ (2^{\alpha-5})$$

b) $x \equiv y \equiv 1\ (2)$

$b_1)$ $b \equiv 2^3 K_1,\ D \equiv 1 + 2^3 K_2,\ x^2 \equiv 1 + 2^3 K_3,\ y^2 \equiv 1 + 2^3 K_4$.

Für K_3 gilt: $K_3 \equiv K_1 + K_2 + K_4 + 2^3 K_2 K_4\ (2^{\alpha-3})$.

$b_2)$ $b=-2+2^3 K_1$, $D=3+2^3 K_2$, $x^2=1+2^3 K_3$, $y^2=1+2^3 K_4$
Für K_3 gilt: $K_3 \equiv K_1+K_2+3K_4+2^3 K_2 K_4 \; (2^{\alpha-3})$.

$b_3)$ $b=4+2^3 K_1$, $D=-3+2^3 K_2$, $x^2=1+2^3 K_3$, $y^2=1+2^3 K_4$
Für K_3 gilt: $K_3 \equiv 1+K_1+K_2+5K_4+2^3 K_2 K_4 \; (2^{\alpha-3})$.

$b_4)$ $b=2+2^3 K_1$, $D=-1+2^3 K_2$, $x^2=1+2^3 K_3$, $y^2=1+2^3 K_4$
Für K_3 gilt: $K_3 \equiv K_1+K_2-K_4+2^3 K_2 K_4 \; (2^{\alpha-3})$.

c) $x \equiv 2\ (4)$, $y \equiv 0\ (4)$

$b=4+2^4 K_1$, $D=1+2K_2$, $x^2=4+2^5 K_3$, $y^2=2^4 K_4^2$ mit $K_1+K_4^2 \equiv 0\ (2)$.
(Letztere Bedingung ist bei beliebigem K_1 durch entsprechende Wahl von y^2 stets erreichbar).

Für K_3 gilt: $K_3 \equiv 1/2 \cdot (K_1+K_4^2)+K_2 K_4^2 \; (2^{\alpha-5})$.

In den Fällen *a, b, c* ist demnach mod 2^α stets eine gewünschte Darstellung möglich; bei den nun folgenden Fällen ist dies nur in Einzelfällen erreichbar.

d) $x \equiv 0\ (4)$, $y \equiv 0\ (4)$

$$b=2^4 K_1,\ D=1+2K_2,\ x^2=2^4 K_3^2,\ y^2=2^4 K_4^2$$

Für K_3 gilt dabei: $K_3^2 \equiv K_1+K_4^2+2K_2 K_4^2 \; (2^{\alpha-4})$

Damit hier K_3, also eine Darstellung, existiert, muss die rechte Seite entweder $\equiv 4\ (8)$ oder $\equiv 1\ (8)$ sein.

e) $x \equiv 0\ (4)$, $y \equiv 2\ (4)$

$b=4+2^3 K_1$, $D=1+2K_2$, $x^2=2^4 K_3^2$, $y^2=4+2^5 K_4$ mit $K_1+K_2 \equiv 1\ (2)$.
Für K_3 gilt: $K_3^2 \equiv 1/2 \cdot (1+K_1+K_2)+2K_4 \, (1+2K_2) \; (2^{\alpha-4})$.
Auch hier gilt dieselbe Anmerkung wie unter *d)*.

II: Fall:

b ungerade, *D* gerade
modulo 8 sind folgende Kombinationen möglich:

x	y	b	D
1 (2)	0 (4)	1 (8)	0 (2)
1 (2)	2 (4)	1 (8)	0 (2)
1 (2)	1 (2)	1 (8)	0 (8)
		−1 (8)	2 (8)
		5 (8)	4 (8)
		3 (8)	−2 (8)

a) $x \equiv 1\ (2),\ y \equiv 0\ (4)$

$b = 1 + 2^3 K_1,\ D = 2 K_2,\ x^2 = 1 + 2^3 K_3,\ y^2 = 2^4 K_4^2$

Für K_3 gilt: $K_3 \equiv K_1 + 4 K_2 K_4^2\ (2^{\alpha-3})$

b) $x \equiv 1\ (2),\ y \equiv 2\ (4)$

$b = 1 + 2^3 K_1,\ D = 2 K_2,\ x^2 = 1 + 2^3 K_3,\ y^2 = 4 + 2^5 K_4$

Für K_3 gilt: $K_3 \equiv K_1 + K_2 + 4 K_2 K_4\ (2^{\alpha-3})$.

c) $x \equiv 1\ (2),\ y \equiv 1\ (2)$

$c_1)$ $b = 1 + 2^3 K_1,\ D = 2^3 K_2,\ x^2 = 1 + 2^3 K_3,\ y^2 = 1 + 2^3 K_4$

Für K_3 gilt: $K_3 \equiv K_1 + K_2\ (1 + 2^3 K_4)\ (2^{\alpha-3})$.

$c_2)$ $b = -1 + 2^3 K_1,\ D = 2 + 2^3 K_2,\ x^2 = 1 + 2^3 K_3,\ y^2 = 1 + 2^3 K_4$

Für K_3 gilt: $K_3 \equiv K_1 + K_2 + 2K_4\ (1 + 4 K_2)\ (2^{\alpha-3})$.

$c_3)$ $b = 5 + 2^3 K_1,\ D = 4 + 2^3 K_2,\ x^2 = 1 + 2^3 K_3,\ y^2 = 1 + 2^3 K_4$

Für K_3 gilt: $K_3 \equiv 1 + K_1 + K_2 + 4 K_4 + 8 K_2 K_4\ (2^{\alpha-3})$.

$c_4)$ $b = 3 + 2^3 K_1,\ D = -2 + 2^3 K_2,\ x^2 = 1 + 2^3 K_3,\ y^2 = 1 + 2^3 K_4$

Für K_3 gilt: $K_3 \equiv K_1 + K_2 - 2 K_4 + 8 K_2 K_4\ (2^{\alpha-3})$.

Im Fall II sind also die modulo 8 möglichen Kombinationen auch nach jeder höheren Potenz von 2 möglich.

III. Fall:

b gerade, *D* gerade

modulo 8 sind folgende Kombinationen möglich:

x	y	b	D
0 (4)	0 (4)	0 (16)	0 (2)
0 (4)	2 (4)	0 (8)	0 (2)
2 (4)	0 (4)	4 (32)	0 (2)
2 (4)	2 (4)	4 (8)	0 (8)
0 (4)	1 (2)	$-D$ (16)	0 (2)
2 (4)	1 (2)	4 (8)	0 (8)
		2 (8)	2 (8)
		0 (8)	4 (8)
		6 (8)	6 (8)

a) $x\equiv 0\ (4),\ y\equiv 0\ (4)$

$b=2^4 K_1,\ D=2 K_2,\ x^2=2^4 K_3^2,\ y^2=2^4 K_4^2$

Für K_3 gilt: $K_3^2\equiv K_1+2 K_2 K_4^2\ (2^{\alpha-4})$.

b) $x\equiv 0\ (4),\ y\equiv 2\ (4)$

$b=2^3 K_1,\ D=2 K_2,\ x^2=2^4 K_3^2,\ y^2=4+2^5 K_4$ mit $K_1+K_2\equiv 0\ (2)$

Für K_3 gilt: $K_3^2\equiv 1/2\cdot(K_1+K_2)+4 K_2 K_4\ (2^{\alpha-4})$.

c) $x\equiv 2\ (4),\ y\equiv 0\ (4)$

$b=4+2^5 K_1,\ D=2 K_2,\ x^2=4+2^5 K_3,\ y^2=2^4 K_4^2$

Für K_3 gilt: $K_3\equiv K_1+K_2 K_4^2\ (2^{\alpha-5})$.

d) $x\equiv 2\ (4),\ y\equiv 2\ (4)$

$b=4+2^3 K_1,\ D=2 K_2,\ x^2=4+2^5 K_3,\ y^2=4+2^5 K_4$ mit $K_1+K_2\equiv 0\ (4)$

Für K_3 gilt: $K_3\equiv 1/4\cdot(K_1+K_2)+4 K_2 K_4\ (2^{\alpha-5})$.

e) $x\equiv 0\ (4),\ y\equiv 1\ (2)$

$b=-D+2^4 K_1,\ D=0\ (2)=2 K_2,\ x^2=2^4 K_3,\ y^2=1+2^3 K_4$

Für K_3 gilt: $K_3^2\equiv K_1+K_2 K_4\ (2^{\alpha-4})$.

f) $x\equiv 2\ (4),\ y\equiv 1\ (2)$

f$_1$) $b=4+2^3 K_1,\ D=2^3 K_2,\ x^2=4+2^5 K_3,\ y^2=1+2^3 K_4$ mit $K_1+K_2\equiv 0\ (4)$

Für K_3 gilt: $K_3\equiv 1/4\cdot(K_1+K_2)+2 K_2 K_4\ (2^{\alpha-5})$.

f$_2$) $b=2+2^3 K_1,\ D=2+2^3 K_2,\ x^2=4+2^5 K_3,\ y^2=1+2^3 K_4$ mit $K_1+K_2\equiv 0\ (4)$

Für K_3 gilt: $K_3\equiv 1/4\cdot(K_1+K_2)+1/2\cdot K_4+2 K_2 K_4\ (2^{\alpha-5})$.

f$_3$) $b=2^3 K_1,\ D=4+2^3 K_2,\ x^2=4+2^5 K_3,\ y^2=1+2^3 K_4$ mit $K_1+K_2\equiv 0\ (4)$

Für K_3 gilt: $K_3\equiv 1/4\cdot(K_1+K_2)+K_4+2 K_2 K_4\ (2^{\alpha-5})$.

f$_4$) $b=6+2^3 K_1,\ D=6+2^3 K_2,\ x^2=4+2^5 K_3,\ y^2=1+2^3 K_4$ mit $K_1+K_2\equiv 3\ (4)$

Für K_3 gilt: $K_3\equiv 1/4\cdot(1+K_1+K_2)+3/2\cdot K_4+2 K_2 K_4\ (2^{\alpha-5})$.

Haben b und D die Gestalt wie bei den Fällen *c*), *d*) und *f*) mit den angegebenen Nebenbedingungen, so existiert stets eine Darstellung modulo 2^α, während für die übrigen Fälle die Bemerkung im Fall I, *d*), zu beachten ist.

LITERATUR

[1] P. BRONKHORST Korrel CXLI: *Een eigenschap van een rekenkundige rij.* Euclides 43 (1967/68), p. 266, Groningen.

[2] WINOGRADOW: *Elemente der Zahlentheorie,* p. 62 ff. Verlag Oldenbourg 1956.