Proof. If P does not equal 1 the result is immediate on putting D equal 1 in the theorem. If P equals 1 then $\mathscr{A}$ must be $\{\langle 0, 1\rangle\}$ and the result still holds. ∎

Now let $\mathscr{A}$ be a collection of AP's, not necessarily regular, which covers the integers. Znám ([5]) defines an AP $\langle a_0, d_0\rangle$ in $\mathscr{A}$ as *essential* if $\mathscr{A}\setminus\langle a_0, d_0\rangle$ does not cover the integers. The following result extends Theorem 1 of [5].

COROLLARY 3. *If $\mathscr{A}$ covers the integers, $\langle a_0, d_0\rangle$ is essential in $\mathscr{A}$, then*

$$|\{\langle a, d\rangle\in\mathscr{A}\colon (d, d_0) > 1\}| \geqslant f(d_0)+1.$$

Proof. Let $\mathscr{A}^*$ be a regular subcollection of $\mathscr{A}$, and P the least common multiple of the moduli of the AP's in it. It is clear that $\langle a_0, d_0\rangle$ belongs to $\mathscr{A}^*$ and hence that d_0 divides P. Then

$$|\{\langle a, d\rangle\in\mathscr{A}\colon (d, d_0) > 1\}| \geqslant \left|\left\{\langle a, d\rangle\in\mathscr{A}^*\colon d\nmid\frac{P}{d_0}\right\}\right| \geqslant f(d_0)+1. \ \blacksquare$$

Acknowledgement. The author wishes to thank Dr. J. Pitman for her unrelenting assistance in the preparation of this paper.

References

[1] I. Korec, *On a generalization of Mycielski's and Znám's conjectures about coset decomposition of Abelian groups*, Fund. Math. 85 (1974), pp. 41–48.

[2] Š. Znám, *On Mycielski's problem on systems of arithmetic sequences*, Colloq. Math. 15 (1966), pp. 201–204.

[3] – *A remark to a problem of J. Mycielski on arithmetic sequences*, ibid. 20 (1969), pp. 69–70.

[4] – *On exactly covering systems of arithmetic sequences*, Colloquia Math. Soc. János Bolyai, 2. Number Theory, Debrecen 1968.

[5] – *On properties of systems of arithmetic sequences*, Acta Arith. 26 (1975), pp. 279–283.

THE UNIVERSITY OF ADELAIDE
G.P.O. Box 498, Adelaide
S. A. 5001, Australia

Received on 5.10.1983
and in revised form on 20.3.1984 (1375)

ACTA ARITHMETICA
XLV (1985)

Verzichtbare und unverzichtbare Elemente bei der Darstellung als Summe und als Differenz von Quadraten

von

ERHARD DEINERT, ERICH HÄRTTER und JOACHIM ZÖLLNER (Mainz)

Wir bezeichnen die Menge der Quadrate der ganzen Zahlen mit Q_0. Nach einem bekannten Satz von Lagrange ist jede natürliche Zahl als Summe von vier Elementen aus Q_0 darstellbar. In [3] wurde gezeigt, daß es unendliche Mengen $S\subset Q_0$ gibt, so daß jede natürliche Zahl auch noch als Summe von vier Quadraten aus $Q_0\setminus S$ darstellbar ist. Erdös und Nathanson [2] haben darüber hinaus die Existenz von Mengen S mit dieser Eigenschaft und $|(Q_0\setminus S)\cap[0, x]|\leqslant Cx^{3/8+\varepsilon}$ für beliebiges $\varepsilon > 0$ nachgewiesen, wobei $C > 0$ nur von ε abhängt(1). In der vorliegenden Arbeit werden genau die Quadrate bestimmt, die in jedem Fall in $Q_0\setminus S$ noch enthalten sein müssen. Solche Quadrate nennen wir unverzichtbar.

Sei Q die Menge der Quadrate der natürlichen Zahlen. Genau die von 1 und 4 verschiedenen natürlichen Zahlen, die $\not\equiv 2 \pmod 4$ sind, lassen sich als Differenz zweier Quadrate aus Q darstellen. In [3] wurde gezeigt, daß dies auch noch mit den Quadraten aus $Q\setminus T$ möglich ist, wobei $T\subset Q$ eine geeignete unendliche Menge von Quadraten ist. Auch in diesem Fall werden die unverzichtbaren Quadrate charakterisiert.

1. Zunächst führen wir einige Bezeichnungen ein(2):

Sei $E(n^2)$ die Menge aller $z\in N_0$, für die gilt: Aus $z = a_1^2+a_2^2+a_3^2+a_4^2$ mit $a_i\in N_0$ $(i = 1, 2, 3, 4)$ folgt $a_i^2 = n^2$ für mindestens ein i.

Sei weiter $U := \{n^2|\ E(n^2)\neq\emptyset\}$ und $\bar{U} := \{n^2|\ |E(n^2)| = \infty\}$.

Sei analog $E^-(n^2)$ die Menge aller $z\in N$, für die gilt: Aus $z = a_1^2-a_2^2$ mit $a_i\in N$ $(i = 1, 2)$ folgt $a_i^2 = n^2$ für $i = 1$ oder für $i = 2$.

Entsprechend wie oben sei dann $U^- := \{n^2|\ E^-(n^2)\neq\emptyset\}$ und $\bar{U}^- := \{n^2|\ |E^-(n^2)| = \infty\}$.

(1) Nathanson [5] zeigte, daß sogar $|(Q_0\setminus S)\cap[0, x]|\leqslant Cx^{1/3+\varepsilon}$ gilt.

(2) N ist die Menge der natürlichen Zahlen; $N_0 = N\cup\{0\}$ die Menge der nichtnegativen ganzen Zahlen.

Dann werden wir folgende Sätze zeigen:

SATZ 1. $U = \{n^2 \mid n = 0, 5, 2^m \text{ oder } 2^m \cdot 3 \text{ mit } m \in N_0\}$.

SATZ 2. $\tilde{U} = \{0^2\}$.

SATZ 3. $U^- = \left\{ n^2 \mid n = \frac{p \pm 1}{2}, \frac{p^2 \pm 1}{2}, p \pm 1 \text{ oder } p^2 \pm 1 \text{ mit } 2 < p \text{ Primzahl} \right\}$.

SATZ 4. $\tilde{U}^- = \emptyset$.

Die unverzichtbaren Quadrate (und damit auch die verzichtbaren Quadrate) sind damit in beiden Fällen charakterisiert.

2. Zum Beweis der Sätze 1 und 2 benötigen wir zunächst einige Vorbereitungen. Es gilt folgender bekannter

SATZ 5 ([3]). *$n \in N_0$ ist genau dann als Summe von 3 Quadraten darstellbar, wenn $n \neq 4^a(8b+7)$ für alle $a, b \in N_0$ gilt.*

Wir zeigen weiter

LEMMA 1. *Es sei $z \in N$, $4|z$, $n^2 \in Q_0$; dann gilt $z \in E(n^2)$ genau dann, wenn $8|z$, $2|n$ und $z/4 \in E((n/2)^2)$.*

Beweis. Sei zuerst $z \in E(n^2)$. Wegen $4|z$ gibt es Zahlen $a_i \in N_0$, $i = 1, 2, 3, 4$, mit $z/4 = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Also ist

$$z = (2a_1)^2 + (2a_2)^2 + (2a_3)^2 + (2a_4)^2. \tag{1}$$

Wegen $z \in E(n^2)$ folgt $2a_i = n$ für ein $i \in \{1, 2, 3, 4\}$, also $2|n$ und $a_i = n/2$ für dieses i. Damit ist $z/4 \in E((n/2)^2)$. Wir nehmen an $8 \nmid z$. Da $4|z$, folgt $z - 1 \equiv 3 \pmod 8$. Nach Satz 5 ist dann $z - 1 = b_1^2 + b_2^2 + b_3^2$ für gewisse $b_1, b_2, b_3 \in N_0$. Aus $z - 1 \equiv 3 \pmod 8$ folgt auch, daß b_1, b_2 und b_3 ungerade sein müssen. Also ist $z = b_1^2 + b_2^2 + b_3^2 + 1^2$, und jedes der vier Quadrate ist ungerade und daher ungleich n^2. Das widerspricht $z \in E(n^2)$. Also gilt $8|z$.

Sei nun umgekehrt $8|z$, $2|n$ und $z/4 \in E((n/2)^2)$. Wegen $8|z$ hat z nur Darstellungen der Form (1). Damit ist $z/4 = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Aus $z/4 \in E((n/2)^2)$ folgt nun $z \in E(n^2)$.

Für $n \in N_0$ sei X_n die Menge aller $x \in N_0$, für die gilt:

$$\begin{aligned} n^2 + x^2 &= a_1^2 + a_2^2, \\ 2n^2 + x^2 &= b_1^2 + b_2^2 + b_3^2, \\ 3n^2 + x^2 &= c_1^2 + c_2^2 + c_3^2 + c_4^2 \end{aligned} \tag{2}$$

mit $a_i, b_j, c_k \in N_0 \setminus \{n\}$.

LEMMA 2. *Sei $n^2 \in Q_0$. Existiert zu $x \in X_n$, $x \neq n$ ein $z \in N_0$, $z \geqslant x^2$ so, daß $z - x^2$ als Summe von drei Quadraten aus Q_0 darstellbar ist, so gilt $z \notin E(n^2)$.*

Beweis. Es gilt also $z = x^2 + x_1^2 + x_2^2 + x_3^2$ für gewisse $x_i \in N_0$, $i = 1, 2, 3$. Ist $x_i \neq n$ für $i = 1, 2, 3$, so haben wir eine Darstellung von z ohne n^2 als Summanden. Für die übrigen Fälle erhalten wir nach Definition von X_n die folgenden Darstellungen von z, in denen n^2 nicht als Summand auftritt:

$$\begin{aligned} &x_1 = n,\ x_2 \neq n \neq x_3; && z = x^2 + n^2 + x_2^2 + x_3^2 = a_1^2 + a_2^2 + x_2^2 + x_3^2; \\ &x_1 = x_2 = n,\ x_3 \neq n; && z = x^2 + 2n^2 + x_3^2 = b_1^2 + b_2^2 + b_3^2 + x_3^2; \\ &x_1 = x_2 = x_3 = n; && z = x^2 + 3n^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2. \end{aligned}$$

Also ist $z \notin E(n^2)$. Damit ist Lemma 2 bewiesen.

LEMMA 3. *Seien $d, z \in N$ und sei*

$$R^{(d)}(z) := \left| \{ \{x, y\} \subseteq N_0 \mid x^2 + dy^2 = z \} \right|,$$

also die Anzahl der wesentlich verschiedenen Darstellungen von z durch die Form $x^2 + dy^2$, so gilt:

(a) *$R^{(1)}(z) \geqslant 2$ genau dann, wenn z mindestens zwei (nicht notwendig verschiedene) Primfaktoren $\equiv 1 \pmod 4$ besitzt und $x, y \in N_0$ existieren mit $z = x^2 + y^2$.*

(b) *Sei $z = 2^\alpha p_1 p_2 \dots p_r u^2$, wobei $\alpha \in N_0$, $2 \nmid u \in N$ und die p_i die sämtlichen Primfaktoren $\equiv 1$ oder $3 \pmod 8$ von z seien (wobei auch gleiche zugelassen sind), so gilt:*

$$R^{(2)}(z) \geqslant 3 \quad \text{genau dann, wenn} \quad \begin{cases} r \geqslant 4, & \text{falls } p_1 = p_2 = \dots = p_r, \\ r \geqslant 3 & \text{sonst.} \end{cases}$$

Der Beweis ergibt sich unmittelbar aus Dickson [1], § 40, Theorem 68 und Problem 1.

LEMMA 4. *Sei $0 \neq z = x^2 + y^2$ mit $x, y \in N_0$ und $2 \nmid x$ oder $2 \nmid y$. Es gelte ferner*

(i) *$p^2 | z$ für eine Primzahl $p \equiv 1 \pmod 4$ oder*

(ii) *$5|z$, $z > 10$ und aus $p | \mathrm{ggT}(x, y)$, p prim folgt $p \equiv 1 \pmod 4$.*

Dann ist $R^{(1)}(z) \geqslant 2$.

Beweis. Gilt (i), so erhält man die Behauptung aus Lemma 3, Teil (a). Es gelte nun (ii). Sei $p|z$ für eine ungerade Primzahl p. Gilt $p \nmid y$, so ist wegen $p|z$ die Kongruenz $x^2 + y^2 \equiv 0 \pmod p$ in x lösbar. Es folgt $\left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right) = 1$, also $p \equiv 1 \pmod 4$. Ist aber $p|y$, dann folgt $p | z - y^2 = x^2$, also $p | \mathrm{ggT}(x, y)$ und es gilt ebenfalls $p \equiv 1 \pmod 4$. Die ungeraden Primfaktoren von z sind also alle $\equiv 1 \pmod 4$. Wegen $2 \nmid x$ oder $2 \nmid y$ tritt der Faktor 2 in z höchstens einmal auf. Da $z/5 > 2$, besitzt $z/5$ mindestens einen Primfaktor $\equiv 1 \pmod 4$, also z mindestens deren zwei. Aus Lemma 3, Teil (a) folgt $R^{(1)}(z) \geqslant 2$.

LEMMA 5. *Sei $0 \neq z = x^2 + 2y^2$ mit $x, y \in N_0$ und $2 \nmid x$ oder $2 \nmid y$, sowie $9|z$, $z > 54$ und aus $p | \mathrm{ggT}(x, y)$, p prim, folgt $p \equiv 1$ oder $3 \pmod 8$; dann gilt $R^{(2)}(z) \geqslant 3$.*

Beweis. Analog zum Beweis von Lemma 4 folgt, daß z nur Primfak-

([3]) Siehe etwa Landau [4], S. 122–123.

toren $\equiv 1$ oder $3 \pmod 8$ und höchstens einmal den Faktor 2 enthält. Wegen $z/9 > 6$ enthält $z/9$ mindestens einen weiteren Primfaktor $\equiv 1$ oder $3 \pmod 8$. Sind alle ungeraden Primfaktoren von $z/9$ gleich 3, dann folgt aus $z/9 > 3 \cdot 2$, daß $3^2 | (z/9)$, also $3^4 | z$. Andernfalls besitzt z mindestens drei ungerade Primfaktoren, die nicht alle gleich sind. Mit Lemma 3, Teil (b) erhalten wir in beiden Fällen $R^{(2)}(z) \geqslant 3$.

LEMMA 6. *Sei t ungerade, $t \neq 9$ oder sei $t = 10$ oder sei $t = 18$. Dann gibt es in X_t eine gerade Zahl $x_g \neq t$ und eine ungerade Zahl $x_u \neq t$; im Falle $t > 5$ kann man $x_g < t$ und $x_u < t$ wählen.*

Beweis. 1. Fall: Sei t ungerade, $t > 5$ und es existiert eine Primzahl $p | t$ mit $p \equiv 1 \pmod 4$.

Man setze für

$t^2 \equiv$	0	1	4	(mod 5)
$x_u =$	5	13	1	
$x_g =$	10	2	4	

Die folgenden Aussagen gelten für jedes $x \in \{x_u, x_g\}$. Für $z = t^2 + x^2$ sind dann die Bedingungen von Lemma 4 (ii) erfüllt, und es gilt $R^{(1)}(z) \geqslant 2$. Also existiert eine weitere Darstellung $z = a^2 + b^2$, $a, b \in N_0$ mit $a \neq t \neq b$. Der kleinst mögliche Wert für t ist in diesem Fall 13 mit $t^2 \equiv 13^2 \equiv 4 \pmod 5$. Also gilt für alle t, daß $x < t$.

Wegen $p^2 | 2t^2$ erhält man aus Lemma 3, Teil (a), daß $R^{(1)}(2t^2) \geqslant 2$. Damit ist $2t^2 = c^2 + d^2$, $c, d \in N_0$ mit $c \neq t \neq d$. Wir haben gezeigt

$$t^2 + x^2 = a^2 + b^2,$$
$$2t^2 + x^2 = c^2 + d^2 + x^2,$$
$$3t^2 + x^2 = a^2 + b^2 + c^2 + d^2,$$

wobei alle Quadrate auf den rechten Seiten dieser Gleichungen von t^2 verschieden sind.

2. Fall: Sei t ungerade und für alle Primfaktoren p von t gelte $p \equiv 3 \pmod 4$, und darüber hinaus sei $t \neq 1, 3, 7, 11, 19, 23, 27, 31, 33, 49$ und 59.

Man setze für

(3)

$t^2 \equiv$		0	1	4	7	(mod 9)
1 (mod 5)	$(x_u, x_g) =$	(3, 12)	(13, 32)	(17, 8)	(97, 2)	
4 (mod 5)		(39, 6)	(41, 4)	(1, 26)	(29, 16)	

Falls $t > 97$, ist $x_u < t$ und $x_g < t$. Auch für die übrigen in diesem Fall betrachteten Werte von t trifft das zu, wie man aus (3) entnehmen kann. Dort erhält man

$t =$	21	43	47	57	63	67	69	71	77	79	81	83	93
$x_u =$	3	1	1	39	39	29	3	13	29	17	3	1	39
$x_g =$	12	26	26	6	6	16	12	32	16	8	12	26	6.

x_u und x_g sind so gewählt, daß sie als Primfaktoren höchstens einmal die 3 und des weiteren nur solche $\not\equiv 3 \pmod 4$ besitzen. Es sei wieder x beliebig aus $\{x_u, x_g\}$ zugelassen. Aus (3) folgt auch, daß in jedem Fall $t^2 + x^2 \equiv 0 \pmod 5$ und $2t^2 + x^2 \equiv 0 \pmod 9$ gilt. Wegen $t \geqslant 11$ ist $121 < t^2 + x^2 < 2t^2 + x^2$. Für $3 \nmid \mathrm{ggT}(t, x)$ ist die Bedingung (ii) von Lemma 4 für $z := t^2 + x^2$ erfüllt. Desgleichen für $z/9$, falls $3 | \mathrm{ggT}(t, x)$, denn $10 < 121/9 < z/9 = (t/3)^2 + (x/3)^2$, und wegen $3 \nmid (x/3)$ ist $3 \nmid \mathrm{ggT}(t/3, x/3)$. In beiden Fällen erhalten wir $R^{(1)}(z) \geqslant 2$. Damit gibt es $a_1, a_2 \in N_0$ mit $a_1 \neq t \neq a_2$ und $t^2 + x^2 = a_1^2 + a_2^2$.

Wir betrachten nun $z_1 := 2t^2 + x^2 \equiv 0 \pmod 9$. Die Zahl t hat nur Primfaktoren $\equiv 3 \pmod 4$, so daß $\mathrm{ggT}(t, x) = 1$ oder 3. Damit sind die Voraussetzungen von Lemma 5 erfüllt, und es gilt $R^{(2)}(z_1) \geqslant 3$. Also existieren zwei weitere Darstellungen dieser Form von z_1, die nicht beide t enthalten können. Es gibt also $b_1, b_2 \in N_0$ mit $b_1 \neq t \neq b_2$ und $2t^2 + x^2 = b_1^2 + 2b_2^2$.

Wegen $3t^2 + x_u^2 \equiv 4 \pmod 8$ folgt aus Lemma 1, daß $3t^2 + x_u^2 \notin E(t^2)$. Es gibt also Zahlen $c_i \neq t$, $i = 1, 2, 3, 4$ mit $3t^2 + x_u^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2$. Damit ist $x_u \in X_t$ gezeigt.

Um auch $x_g \in X_t$ nachzuweisen, genügt es, $3t^2 + x_g^2 \notin E(t^2)$ zu zeigen. Es gilt $z_2 := 3t^2 + x_g^2 \equiv 3 \pmod 4$. Wir betrachten $z_2 - x_u^2 \equiv 2 \pmod 4$. Nach Satz 5 besitzt $z_2 - x_u^2$ eine Darstellung als Summe von drei Quadraten. Wegen $z_2 - x_u^2 > t^2 - x_u^2 > 0$ folgt aus Lemma 2, daß $3t^2 + x_g^2 = z_2 \notin E(t^2)$.

3. Fall: $t = 1, 3, 5, 7, 11, 19, 23, 27, 31, 33, 49, 59, 10$ oder 18.

Hier geben wir $x_u, x_g \in X_t$ direkt an. Geeignete $a_i, b_j, c_k \in N_0 \setminus \{t\}$ in den Gleichungen (2) lassen sich dann durch einfache Rechnungen auffinden.

$t =$	1	3	5	7	11	19	23	27	31	33	49	59	10	18
$x_u =$	13	21	15	1	3	3	1	1	1	1	3	3	5	1
$x_g =$	8	16	0	4	2	2	2	4	2	4	2	2	0	4.

Es gilt $x_u \neq t \neq x_g$, und für $t > 5$ ist $x_u < t$, $x_g < t$ erfüllt.

SATZ 6. *Sei $t \in N$, $4 \nmid t$ und $n = 2^r t$ mit $r \in N_0$. Existieren $x_u, x_g \in X_t$ mit $2 \nmid x_u \neq t$, $2 | x_g \neq t$, so folgt aus $z > \max((2^r x_u)^2, (2^r x_g)^2)$, daß $z \notin E(n^2)$.*

Beweis. Für $z \in N_0$, $z < n^2$ gilt trivialerweise $z \notin E(n^2)$. Sei also $z \geqslant n^2$.

1. Fall: $z - (2^r x_u)^2$ oder $z - (2^r x_g)^2$ ist als Summe dreier Quadrate darstellbar. Für ein $x \in \{x_u, x_g\}$ sei dies zutreffend. Multipliziert man die Gleichungen (2) mit $(2^r)^2$, so erhält man $2^r x \in X_{2^r t} = X_n$. Mit Lemma 2 folgt $z \notin E(n^2)$, da aus $x_u \neq t \neq x_g$ folgt $n = 2^r t \neq 2^r x$.

2. Fall: $z-(2^r x_u)^2$ und $z-(2^r x_g)^2$ sind nicht als Summen von drei Quadraten darstellbar. Nach Satz 5 gilt dann mit gewissen $a, b, c, d \in N_0$

$$z-(2^r x_u)^2 = 4^a(8b+7), \tag{4}$$

$$z-(2^r x_g)^2 = 4^c(8d+7). \tag{5}$$

Aus diesen Gleichungen folgt

$$4^{r'}(x_g^2-x_u^2) = 4^{a'}(8b+7)-4^{c'}(8d+7), \tag{6}$$

wobei wenigstens eine der Zahlen $r', a', c' \in N_0$ gleich 0 sei.

Ist $r'=0$, so gilt $3 \equiv x_g^2-x_u^2 = 4^{a'}(8b+7)-4^{c'}(8d+7) \pmod 4$. Damit ist $a'=0$ und $c'>0$ und es gilt $a=r$. Aus (4) folgt $z' := z/4^r = 8b+7+x_u^2 \equiv 0 \pmod 8$, da $x_u^2 \equiv 1 \pmod 8$. Sei $x_g = 2^m s$ mit $m \in N$, $2 \nmid s \in N$ oder $s=0$. Aus (5) folgt

$$z' = z/4^r = 4^{c'}(8d+7)+4^m s^2. \tag{7}$$

Ist $s=0$, so folgt wegen $8|z'$, daß $c' \geqslant 2$, also $16|z'$.

Nun sei $s>0$. Für $\min(c', m) \geqslant 2$ folgt aus (7) sofort $16|z'$. Ist $\min(c', m) = 1$, so ist $c' \neq m$ unmöglich, denn nach (7) würde gelten $8 \nmid z'$. Damit ist $c' = m = 1$. Aus (7) folgt nun $z' = 4(8d+7+s^2) \equiv 0 \pmod{32}$, da $s^2 \equiv 1 \pmod 8$. In jedem Fall ist $16|z' = z/4^r$, also $4|(z/4^{r+1})$. Wäre $z \in E(n^2)$, so würde durch $(r+1)$-fache Anwendung von Lemma 1 folgen, daß $2|t$ und $z/4^{r+1} \in E\big((n/2^{r+1})^2\big) = E\big((t/2)^2\big)$. Da $4|(z/4^{r+1})$, würde durch nochmalige Anwendung $2|(t/2)$ folgen, also $4|t$, im Widerspruch zur Voraussetzung. Somit gilt $z \notin E(n^2)$.

Sei nun $r'>0$. Damit muß $a'=0$ oder $c'=0$ sein. Aus (6) folgt dann sofort, $a'=c'=0$. Also ist $a=c$ und man hat $r-a=r'>0$. Aus (5) folgt wegen $2|x_g$, daß $z/4^a = 8d+7+4^{r'}x_g^2 \equiv 7 \pmod 8$. Damit erhalten wir aus $z/4^a = y_1^2+y_2^2+y_3^2+y_4^2$, $y_i \in N_0$, $i=1, 2, 3, 4$, daß o.B.d.A. gilt $y_1^2 \equiv y_2^2 \equiv y_3^2 \equiv 1 \pmod 8$, $y_4^2 \equiv 4 \pmod 8$. Wir betrachten nun $z = (2^a y_1)^2+(2^a y_2)^2+(2^a y_3)^2+(2^a y_4)^2$. Wegen $a<r$ und $2 \nmid y_i$ für $i=1, 2, 3$ folgt $2^a y_i \neq 2^r t = n$ für $i=1, 2, 3$. Wir nehmen an, es gilt $2^a y_4 = n = 2^r t$. Es ist $y_4 \equiv 2 \pmod 4$, so daß wegen $a<r$ gelten muß $r=a+1$ und $r'=1$. Aus (4) folgt dann der Widerspruch $7 \equiv z/4^a = 8b+7+4x_u^2 \equiv 3 \pmod 8$. Damit ist $2^a y_i \neq n$ für $i=1, 2, 3, 4$. Daher folgt auch diesmal $z \notin E(n^2)$.

Es gilt noch der folgende

Satz 7 (siehe Sierpiński [6], S. 373).

$$E(0^2) = \{0, 1, 3, 5, 9, 11, 17, 29, 41, 2^{2k+1}, 2^{2k+1}\cdot 3, 2^{2k+1}\cdot 7 \mid k \in N_0\}.$$

Nun zum

Beweis von Satz 1 und Satz 2. Nach Lemma 6 gibt es für alle ungeraden t, $t \neq 9$, sowie für $t=10$ und $t=18$ Zahlen $x_u, x_g \in X_t$ mit $2 \nmid x_u \neq t$, $2|x_g \neq t$. Zu jedem $n \in N$, $n \neq 9$ kann eines dieser t gewählt werden mit $n = 2^r t$, $r \in N_0$. Wegen $4 \nmid t$ folgt aus Satz 6 für alle $z \in E(n^2)$, daß

$z \leqslant \max\big((2^r x_u)^2, (2^r x_g)^2\big)$. Damit ist $|E(n^2)| < \infty$. Für ungerade $t>5$, sowie für $t=10$ und $t=18$ gilt nach Lemma 6 darüber hinaus $z \leqslant \max\big((2^r x_u)^2, (2^r x_g)^2\big) < (2^r t)^2 = n^2$. Da aber $z \geqslant n^2$ sein muß, ist $E(n^2) = \emptyset$ für alle $n \in N$ mit $n \neq 2^k, 2^k\cdot 3, 5, 9$ $(k \in N_0)$. Nun zeigen wir, daß auch $E(9^2) = \emptyset$ ist. Sei $z \in E(9^2)$. Da, wie soeben bewiesen, $E(18^2) = \emptyset$ ist, kann z nach Lemma 1 nicht gerade sein. Sei also $z \equiv 1, 3, 5$ oder $7 \pmod 8$. Es gilt wegen

$$\begin{aligned} 9^2+2^2 &= 7^2+6^2, & & 9^2+8^2 = 12^2+1^2, \\ 2\cdot 9^2+2^2 &= 11^2+6^2+3^2, & \text{bzw.} \quad & 2\cdot 9^2+8^2 = 15^2+1^2+0^2, \\ 3\cdot 9^2+2^2 &= 15^2+3^2+3^2+2^2, & & 3\cdot 9^2+8^2 = 17^2+3^2+3^2+0^2, \end{aligned}$$

daß $2 \in X_9$ und $8 \in X_9$. Da $z \geqslant 9^2$ ist, gilt mit geeigneten $x \in \{2, 8\}$, daß $0 < z-x^2 \not\equiv 7 \pmod 8$. Aus Satz 5 und Lemma 2 folgt $z \notin E(9^2)$, also $E(9^2) = \emptyset$. Daher ist $|E(n^2)| < \infty$ für alle $n \in N$. Nach Satz 7 ist $|E(0^2)| = \infty$. Damit folgt Satz 2.

Zum Beweis von Satz 1 muß noch $E(n^2) \neq \emptyset$ für $n = 2^k, 2^k\cdot 3, 5$ $(k \in N_0)$ gezeigt werden.

Zuerst sei $n = 2^k$, $k \in N_0$. Es ist $8/4 = 2 \in E(1^2) = E\big((2/2)^2\big)$. Aus Lemma 1 folgt $8 \in E(2^2)$. Die k-malige Anwendung dieses Lemmas liefert $2^{2k+1} \in E\big((2^k)^2\big)$.

Sei nun $n = 2^k\cdot 3$, $k \in N_0$. Es ist $14 \in E(3^2)$. Wie oben folgt $2^{2k+1}\cdot 7 \in E\big((3\cdot 2^k)^2\big)$.

Schließlich sei $n=5$. Es gilt $79 \in E(5^2)$, denn $49+\underline{25}+4+1 = 36+\underline{25}+9+9 = \underline{25}+\underline{25}+\underline{25}+4$ sind sämtliche wesentlich verschiedenen Darstellungen von 79. Also ist $U = \{0^2, 5^2, (2^k)^2, (2^k\cdot 3)^2 \mid k \in N_0\}$.

Bemerkung. Mit den hier entwickelten Methoden läßt sich für die Fälle mit $E(n^2) \neq \emptyset$ die Menge $E(n^2)$ auch genau angeben, wobei die Berechnung hier nicht ausgeführt ist(4).

Wir formulieren das Ergebnis als

Satz 8.

$$E(1^2) = \{1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 19, 23, 30, 35, 39, 46, 51, 55\},$$

$$E(2^2) = \{5, 6, 7, 8, 13, 14, 15, 21, 22, 23, 24, 29, 30, 31, 40, 56, 120, 184\},$$

$$E\big((2^k)^2\big) = \{2^{2k-1}\cdot x,\ 2^{2k+1}\cdot y \mid x = 3, 7, 11, 15;\ y = 1, 3, 5, 7, 15, 23\}$$

für $k \geqslant 2$,

$$E(3^2) = \{11, 14, 15, 23, 35, 47, 59, 71, 95\},$$

$$E\big((2^k\cdot 3)^2\big) = \{2^{2k+1}\cdot 7\} \quad \textit{für} \quad k \geqslant 1,$$

$$E(5^2) = \{79\}.$$

(4) Man benutzt Gleichungen der Form (2), sowie Satz 6 und Lemma 1. Für die numerischen Rechnungen reicht ein Taschenrechner aus.

3. Wir betrachten nun Darstellungen durch Differenzen von zwei Quadraten und kommen zum Beweis des Satzes 3. Bei diesem Beweis wird gleichzeitig auch der folgende Satz mit bewiesen:

SATZ 9. *Es gilt*

$$E^-(1^2) = \{3, 8\},$$
$$E^-(3^2) = \{5, 7, 8, 16\},$$
$$E^-(5^2) = \{9, 11, 16, 24\}.$$

Für $n \in N$, $n \neq 1, 3, 5$ *gilt*:

$E^-(n^2)$ *ist die Menge der Zahlen* $2n \pm 1$, *die Primzahlen oder Quadrate von solchen sind, sowie der Zahlen* $4(n \pm 1)$, *sofern* $n \pm 1$ *ungerade Primzahl oder Quadrat einer solchen ist.*

Für alle $n \in N$ *ist* $|E^-(n^2)| \leqslant 4$.

Beweis der Sätze 3 und 9. Für $z \in D$ sei

$$g(z) := |\{(a, b) \in N^2 |\ z = a^2 - b^2\}|.$$

Dann ist nach [6], S. 381

$$g(z) = |\{(d, d') \in N^2 |\ dd' = z,\ d < d',\ d \equiv d' \pmod 2\}|,$$

also

$$g(z) = \begin{cases} [\frac{1}{2}\tau(z)], & \text{falls } z \equiv 1 \pmod 2, \\ [\frac{1}{2}\tau(z/4)], & \text{falls } z \equiv 0 \pmod 4; \end{cases} \tag{8}$$

dabei ist $\tau(x)$ die Anzahl der positiven Teiler von x.

Genau dann ist $n^2 \in U^-$, wenn es ein $z \in D$ mit $z \in E^-(n^2)$ gibt.

Sei nun $z \in D$, $z = a^2 - b^2$ mit $a, b \in N$. Dann unterscheidet man die folgenden drei Fälle:

(a) $g(z) \geqslant 3$. Dann ist $z \notin E^-(a^2)$ und $z \notin E^-(b^2)$.

(b) $g(z) = 2$, $z = a^2 - b^2 = c^2 - d^2$ mit $c, d \in N$, $(a, b) \neq (c, d)$.

Dann gilt:

Aus $a^2 = d^2$ folgt $z \in E^-(a^2)$, $z \notin E^-(b^2)$;

aus $b^2 = c^2$ folgt $z \notin E^-(a^2)$, $z \in E^-(b^2)$;

in den übrigen Fällen ist $z \notin E^-(a^2)$ und $z \notin E^-(b^2)$.

(c) $g(z) = 1$. Dann ist $z \in E^-(a^2)$ und $z \in E^-(b^2)$.

Nach Formel (8) ist $g(z) = 1$ genau dann, wenn

$$z \in \{8, 16, t^2 \cdot p, t^2 \cdot p^2 |\ p \text{ Primzahl}, p > 2, t = 1 \text{ oder } t = 2\}.$$

Dabei ist

$$z = 8 = 3^2 - 1^2, \quad z = 16 = 5^2 - 3^2, \tag{9}$$

$$z = t^2 p^\nu = \left(t\frac{p^\nu + 1}{2}\right)^2 - \left(t\frac{p^\nu - 1}{2}\right)^2 \quad (\nu = 1, 2). \tag{10}$$

Genau dann ist $g(z) = 2$, wenn

$$z \in \{32, 64, t^2 p^3, t^2 p^4, t^2 pq, 8p |\ p, q \text{ Primzahlen}, p > 2, q > 2, p \neq q, t = 1 \text{ oder } t = 2\}.$$

Dabei ist

$$32 = 9^2 - 7^2 = 6^2 - 2^2; \quad 64 = 17^2 - 15^2 = 10^2 - 6^2.$$

Falls $z = t^2 uv$ mit $u \equiv v \equiv 1 \pmod 2$, $u > v \geqslant 3$, so ist

$$z = \left(\frac{t(u+v)}{2}\right)^2 - \left(\frac{t(u-v)}{2}\right)^2 = \left(\frac{t(uv+1)}{2}\right)^2 - \left(\frac{t(uv-1)}{2}\right)^2.$$

Aus

$$\frac{t(u \pm v)}{2} = \frac{t(uv \mp 1)}{2}$$

würde folgen $\pm(v+1) = u(v-1)$, also der Widerspruch

$$2 \geqslant \pm\frac{v+1}{v-1} = u > 3.$$

Für $z = 8p$ gilt

$$8p = (2p+1)^2 - (2p-1)^2 = (p+2)^2 - (p-2)^2.$$

Stets ist $2p+1 > p-2$, und $2p-1 = p+2$ genau für $p = 3$.

Im Fall (b) erhalten wir also nur $24 \in E^-(5^2)$. Damit, sowie mit (9) und (10), folgen nun die Behauptungen der Sätze 3 und 9.

Beweis von Satz 4. Aus Satz 9 folgt insbesondere, daß $E^-(n^2)$ für jedes $n \in N$ endlich ist.

Literaturverzeichnis

[1] L. E. Dickson, *Modern elementary theory of numbers*, Chicago 1939.

[2] P. Erdös, M. B. Nathanson, *Lagrange's theorem and thin subsequences of squares*, in: *Contributions to probability*, New York 1981, S. 3–9.

[3] E. Härtter, J. Zöllner, *Darstellungen natürlicher Zahlen als Summe und als Differenz von Quadraten*, Det Kgl. Norske Vidensk. Selsk. Skr. No. 1, 1977, S. 1–8.

[4] E. Landau, *Vorlesungen über Zahlentheorie, Aus der elementaren Zahlentheorie*, New York 1950.

[5] M. B. Nathanson, *Waring's problem for sets of density zero*, in: *Analytic number theory*, Lecture Notes in Math. No 899, Berlin–Heidelberg–New York 1981, S. 301–310.

[6] W. Sierpiński, *Elementary theory of numbers*, Warszawa 1964.

Eingegangen am 15.11.1983
und in revidierter Form am 9.3.1984 (1382)