ACTA ARITHMETICA
XL (1982)

Ein Sonderfall der diophantischen Gleichung $\frac{x^a-(\pm 1)^a}{x\mp 1}=z^a$

von

B. RICHTER (Berlin)

Bei seinen Untersuchungen mehrfach vollkommener Zahlen benötigt Steuerwald [6] den Satz:

Das Paar diophantischer Gleichungen

$$3^a-1=p^\sigma 2^\alpha,$$

$$2^b-1=p^\tau 3^\beta,$$

$p\neq 2,3$ Primzahl, $a, b, \sigma, \tau, \alpha\in N$, $\beta\in N_0$, besitzt nur die Lösung

$$3^4-1=5\cdot 2^4,$$

$$2^4-1=5\cdot 3.$$

Im selben Zusammenhang habe ich in meiner Dissertation [4] den folgenden Satz bewiesen:

Das Paar diophantischer Gleichungen

$$p_1^a+1=p^\sigma p_2^\alpha,$$

$$p_2^b+1=p^\tau p_1^\beta,$$

p, p_i $(i=1,2)$ paarweise verschiedene Primzahlen, $a, b, \sigma, \tau, \alpha, \beta\in N$, besitzt nur die Lösungen

$$3^2+1=2\cdot 5,\quad 11+1=3\cdot 2^2,\quad 5^2+1=13\cdot 2,$$

$$5+1=2\cdot 3,\quad 2^5+1=3\cdot 11,\quad 2^6+1=13\cdot 5.$$

Ein wichtiges Hilfsmittel dabei war der Satz:

Das (Unter-) System

$$p_1^a+1=2^\sigma p_2^\alpha,$$

$$p_2^b+1=2^\tau p_1^\beta$$

ist mit ungeraden a und b unlösbar.

Dieses Ergebnis habe ich nun wie folgt verallgemeinert, und hoffe, in Zukunft davon Anwendungen geben zu können:

Satz. *Die diophantische Gleichung*

$$(*)\qquad \frac{x^a-y^a}{x-y}=z^a$$

besitzt unter den Nebenbedingungen

$$x-y=cp^\sigma,\qquad z-y'=p^\tau x^\beta$$

mit $a, c, \sigma, \tau, \alpha, \beta, x, z\in \boldsymbol{N}$, $y, y'\in \boldsymbol{Z}$, $|y|=|y'|=1$ *und* p *Primzahl mit* $(c,p)=1$ *sowie*

$$c\leqslant\begin{cases}2p-1, & p,\ a \text{ ungerade},\\ p+1, & p \text{ ungerade},\ a \text{ gerade},\\ 1, & p=2,\end{cases}$$

nur die Lösungen

$$1^a-(-1)^a=2\cdot 1^a,\quad 2^5+1=3\cdot 11,\quad 2^4-1=3\cdot 5,$$
$$a \text{ ungerade}\qquad 11+1=3\cdot 2^2,\quad 5+1=3\cdot 2,$$
$$3^3+1=2^2\cdot 7,\quad 3^3-1=2\cdot 13,\quad 3^5-1=2\cdot 11^2,\quad 7^4-1=6\cdot 20^2,$$
$$7-1=2\cdot 3,\quad 13-1=2^2\cdot 3,\quad 11+1=2^2\cdot 3,\quad 20+1=3\cdot 7.$$

Wie Steuerwald brauchen wir zum Beweis im wesentlichen nur das elementare Ergebnis von Zsigmondy [7] (vgl. [3] und [4]):

(Z) *Sind* $x, y\in \boldsymbol{Z}\setminus\{0\}$ *teilerfremd und* $|xy|\neq 1$, $a\in \boldsymbol{N}\setminus\{1\}$, *so gibt es für jeden Teiler* $d>1$ *von* a *einen ungeraden Primfaktor* q *von* $Q(x,y,a)$ *mit* $d=d_q(x,y)$. *Die einzigen Ausnahmen sind* $d=2$, *falls* $|x+y|=2^v$, $v\in \boldsymbol{N}_0$, $d=3$, *falls* $xy=-2$ *und* $d=6$ *falls* $xy=2$.

Hierbei ist

$$Q(x,y,a)=\frac{x^a-y^a}{x-y}=x^{a-1}+yx^{a-2}+\ldots+y^{a-1}$$

und $d_q(x,y)$ die Ordnung von x und y bzgl. q, d.h.

$$d_q(x,y)=\min\{n\in \boldsymbol{N}|\ x^n\equiv y^n \pmod q\}$$

(für beliebige PZ (Primzahl) q gilt $d_q|q-1$).

Sind $u, v\in \boldsymbol{Z}$, so definieren wir noch

$$u\subset v:\ \Leftrightarrow \forall q \text{ PZ}:\ q|u\Rightarrow q|v.$$

Dann ergeben sich aus (Z) fast unmittelbar die folgenden Sätze (vgl. [3] und [4]):

(P_0) *Ist* $Q(x,y,a)=u\subset x-y$, *so ist*

$$a=u=3,\qquad xy=-2$$

oder

$$a=2,\qquad |x+y|=|u|=2^v,\qquad v\in \boldsymbol{N}_0$$

oder

$$a=u=1.$$

(P_1) *Ist* $Q(x,y,a)=up^a$ *mit* $u\subset x-y$, p PZ, $p\nmid x-y$ *und ist nicht* $3|a$, $xy=-2$ *oder* $2|a$, $|x+y|=2^v$, $v\in \boldsymbol{N}_0$, *so ist* a PZ, $p\equiv 1 \pmod a$.

(P_2) *Ist* $Q(x,y,a)=up_1^{a_1}p_2^{a_2}$ *mit* $u\subset x-y$, p_i *paarweise verschiedene Primzahlen,* $p_i\nmid x-y$ $(i=1,2)$, *und ist nicht* $6|a$, $xy=2$ *oder* $3|a$, $xy=-2$ *oder* $2|a$, $|x+y|=2^v$, $v\in \boldsymbol{N}_0$, *so gibt es eine* PZ q *mit* $a=q$ *oder* q^2, $p_i\equiv 1 \pmod q$ $(i=1,2)$.

Über die Primfaktorzerlegung von $Q(x,y,a)$ wissen wir Bescheid:

(F) *Ist* $x\equiv y \pmod p$, *so ist*

$$\nu_p(Q)=\begin{cases}\nu_p(a) & \text{falls } p \text{ ungerade},\\ \nu_p(x+y)+\nu_p(a)-1 & \text{falls } p=2,\ a \text{ gerade},\\ 0 & \text{falls } p=2,\ a \text{ ungerade}.\end{cases}$$

(vgl. Inkeri [1] sowie [3] und [4]).

Zum Beweis des Satzes betrachte ich allgemein die diophantische Gleichung

$$Q(x,y,a)=z^a$$

unter den Nebenbedingungen

$$\text{(N)}\qquad z-y'=p^\tau x^\beta,\qquad x\equiv y \pmod p,\qquad x\neq y;$$

d.h. ich lasse die Beschränkungen des c durch p weg.

Er ergibt sich dann durch die Kette der folgenden Lemmata.

Bemerkung 1. Wir könnten die Beweisführung (unwesentlich) kürzen, wenn wir das Ergebnis von Ljunggren [2]:

Die diophantische Gleichung $Q(x,1,a)=z^2$ *besitzt für* $a>2$ *und* $x>1$ *nur die Lösungen* $x=3$, $a=5$, $z=11$ *und* $x=7$, $a=4$, $z=20$

benützten. Das würde allerdings der Arbeit den elementaren Charakter nehmen.

In diesem Zusammenhang ist die Arbeit von Shorey und Tijdeman [5] interessant, die u. a. besagt, daß (*) für gerades a und $y = 1$ nur endlich viele Lösungen besitzt.

Bemerkung 2. Erweitern wir den Definitionsbereich auf $x, z \in \boldsymbol{Z}$, so erhält man keine wesentlich anderen Lösungen:

Da $p \geqslant 2$, sind $x, z \neq 0$. Angenommen $z < 0$. Dann ist $x^\beta < 0$, also $x < 0$, β ungerade.

a gerade, dann $(x-y<0)$ $x^a < 0$, also a ungerade, und $-x$, $-y$, $-z$ ist Lösung.

a ungerade, dann $(x-y<0)$ $x^a > 0$, also a gerade, und $-x$, $-y$, $-z$ ist Lösung.

Mithin o.B.d.A. $z > 0$. Angenommen $x < 0$. Dann ist β gerade und $(x-y<0)$ $x^a < 0$. Also a ungerade, und $-x$, $-y$, z ist Lösung.

Wir setzen deshalb weiterhin $x, z \in \boldsymbol{N}$ voraus.

Wegen $2z \geqslant z+1 \geqslant z-y' \geqslant 2x$ ist $z > x$ außer für $x = z = 1$. Ist $x = 1$, dann ist $y = -1$, $p = 2$, a ungerade, $z = 1$, $y' = -1$. Das ist die triviale Lösung von (*).

Sei $x \geqslant 2$. Dann ist $z \geqslant 3$, $a \geqslant 2$. Aus $z \equiv y' \pmod{x}$ folgt

$$y^{a-1} \equiv z^a \equiv y'^a \pmod{x}.$$

Lemma 1. *Es gelte $y^{a-1} = -y'^a$. Die einzige nichttriviale Lösung von* (*) *mit* (N) *ist*

$$2^5+1 = 3\cdot 11, \quad 11+1 = 3\cdot 2^2.$$

Beweis. Es ist $x = 2$, $y = -1$, $p = 3$. Aus $2^a-(-1)^a = 3z^a$ folgt wegen $(p, z) = 1$, daß

$$a, z \geqslant 4, \quad 3z^a \equiv -(-1)^a \pmod{8}.$$

Dann ist a ungerade, sonst

$$z^a \equiv 1 \pmod{8} \Rightarrow 3 \equiv \pm 1 \pmod{8} \Rightarrow \mathrm{W}! \text{ (Widerspruch.)}$$

Für $\beta \geqslant 3$ folgt $z \equiv y' \pmod{8}$, also ebenfalls

$$3 \equiv \pm 1 \pmod{8} \Rightarrow \mathrm{W}!$$

Also ist $\beta = 1, 2$.

Aus $\beta = 1$ folgt $z \equiv -y' \pmod{4} \Rightarrow (-1)^a \equiv z^a \equiv (-y')^a \equiv -y'^a = y^{a-1} \equiv (-1)^{a-1} \pmod{4} \Rightarrow \mathrm{W}!$

Also ist $\beta = 2$, $y' = (-1)^a$.

Wir wenden jetzt die Methode an, die auch nachher zum Erfolg führen wird.

Es ist

$$\begin{aligned} z^a = Q(2, -1, a) &= (-1)^{a-1}+2Q(2, -1, a-1) \\ &= (-1)^{a-1}+2[(-1)^{a-2}+2Q(2, -1, a-2)]. \end{aligned}$$

Also

$$4\cdot Q(2, -1, a-2) = z^a-(-1)^{a-2} = z^a-y'^a = 4\cdot 3^\tau\cdot Q(z, y', a),$$

$$Q(2, -1, a-2) = 3^\tau\cdot Q(z, y', a).$$

Da $2 \equiv -1 \pmod{3}$, $z \equiv y' \pmod{3}$, folgt aus (F), daß

$$\nu_3(a-2) = \tau+\nu_3(a).$$

Nach (Z) gibt es einen ungeraden Primfaktor q von z mit $d_q(2, -1) = a$, $a \mid q-1$. Wir setzen $q-1 = \gamma\lambda a$, $z = rq$ mit

$$\lambda, r \in \boldsymbol{N} \quad \text{und} \quad \gamma = \begin{cases} 2, & a \text{ ungerade}, \\ 1, & a \text{ gerade}. \end{cases}$$

Dann ist

$$\begin{aligned} \gamma r\lambda(a-2) &= \gamma r\lambda a-2\gamma r\lambda = r(q-1)-2\gamma r\lambda \\ &= z-r(1+2\gamma\lambda) = 4\cdot 3^\tau-[r(1+2\gamma\lambda)-y']. \end{aligned}$$

Aus $\nu_3(a-2) \geqslant \tau$ folgt $\nu_3[r(1+2\gamma\lambda)-y'] \geqslant \tau$, also mit gewissen $t, \varrho \in \boldsymbol{N}$

$$a-2 = t\cdot 3^\tau, \quad r(1+2\gamma\lambda)-y' = 2\varrho\cdot 3^\tau, \quad \text{da } r \text{ ungerade}.$$

Da

$$(4-2\varrho)3^\tau = \gamma r\lambda(a-2) > 0, \quad \text{ist} \quad \varrho = 1.$$

Damit ist

$$2 = \gamma r\lambda t.$$

$$\begin{aligned} a \text{ ungerade} &\Rightarrow \gamma = 2 \Rightarrow r = \lambda = t = 1, \\ &\quad 1+4-y' = 2\cdot 3^\tau \Rightarrow y' = -1,\ \tau = 1,\ a = 5, \\ &\quad 2^5+1 = 3\cdot 11,\ 11+1 = 4\cdot 3 \text{ ist Lösung}. \\ a \text{ gerade} &\Rightarrow \gamma = 1,\ t = 2 \Rightarrow r = \lambda = 1, \\ &\quad 1+2-y' = 2\cdot 3^\tau \Rightarrow \mathrm{W}! \end{aligned}$$

In Zukunft sei also $y^{a-1} = y'^a$. Wir nehmen diese Bedingung zu (N) hinzu.

Es ist jetzt

$$z^a = Q(x, y, a) = y^{a-1}+xQ(x, y, a-1).$$

Damit ist

$$xQ(x, y, a-1) = z^a-y'^a = p^\tau x^\beta Q(z, y', a).$$

Da $x \nmid Q(x, y, a-1)$ folgt $\beta = 1$ und

$$(**) \qquad Q(x, y, a-1) = p^\tau Q(z, y', a).$$

Lemma 2. *Sei $a = 1$. Die einzigen nichttrivialen Lösungen von* (*) *mit* (N) *sind*

$$x = 2,\ y = -1,\ a = 4 \quad \textit{und} \quad x+y = 2^\tau,\ a = 3.$$

Beweis. Da $x \equiv y \pmod p$ gibt es nach (P_0) nur die Lösungen

$$x = 2,\ y = -1,\ a-1 = 3 = p^\tau \quad (\text{dann ist } y' = -1,\ z = 5)$$

und

$$x+y = 2^\tau,\ a-1 = 2 \quad (\text{dann ist } y' = 1).$$

LEMMA 3. *Für eine nichttriviale Lösung von* $(*)$ *mit* (N) *ist* $\alpha < a$, $ap^\tau \equiv yy' \pmod x$. *Gilt* $\alpha > 1$, *so ist*

$$2y'[\alpha p^\tau - yy'] \equiv x[1+yy'p^\tau] \pmod{x^2}. \text{ (1)}$$

Beweis. Aus $x^\alpha < z^\alpha < (x-y)z^\alpha + y^\alpha = x^a$ folgt $\alpha < a$. Da

$$Q(z, y', \alpha) = \sum_{k=0}^{\alpha-1} z^k y'^{\alpha-1-k} = \sum_{k=0}^{\alpha-1}\left(\sum_{l=0}^{k}\binom{k}{l}(p^\tau x)^l y'^{k-l}\right) y'^{\alpha-1-k}$$
$$= \sum_{l=0}^{\alpha-1}(p^\tau x)^l y'^{\alpha-1-l}\sum_{k=l}^{\alpha-1}\binom{k}{l} = \sum_{l=0}^{\alpha-1}\binom{\alpha}{l+1}(p^\tau x)^l y'^{\alpha-1-l}$$

ergibt sich aus $(**)$, daß

$$y^{a-2} + xy^{a-3} + x^2\{\ldots\} = p^\tau\left[\alpha y'^{\alpha-1} + \binom{\alpha}{2} p^\tau x y'^{\alpha-2} + x^2\{\ldots\}\right].$$

Also

$$y'^{\alpha-1}[\alpha p^\tau - yy'] \equiv xy'^{\alpha-2}\left[1 - p^{2\tau}\binom{\alpha}{2}\right] \pmod{x^2},$$

d.h.

$$\alpha p^\tau \equiv yy' \pmod x.$$

Dann ist aber

$$2p^{2\tau}\binom{\alpha}{2} = (\alpha p^\tau)^2 - (\alpha p^\tau)p^\tau \equiv 1 - yy'p^\tau \pmod x.$$

LEMMA 4. *Für eine nichttriviale Lösung von* $(*)$ *mit* (N) *ist*

$$\nu_p(a-1)\begin{cases} = \tau + \nu_p(\alpha) & \text{für} \quad p > 2, \\ \geqslant \tau + \nu_p(\alpha) & \text{für} \quad p = 2,\ \nu_p(x-y) > 1 \\ & \qquad \text{oder } x-y = 2,\ \tau = 1,\ \alpha \text{ gerade}, \\ = \tau - 1 + \nu_p(\alpha) & \text{für} \quad p = 2,\ x-y = 2,\ \alpha \text{ ungerade} \\ & \qquad \text{oder } \tau > 1,\ \alpha \text{ gerade}. \end{cases}$$

Beweis. Da $x \equiv y \pmod p$ und $z \equiv y' \pmod p$ folgt aus $(**)$ mit (F), daß

$$\nu_p(a-1) = \tau + \nu_p(\alpha) \quad \text{für } p \text{ ungerade}$$

(1) Eine der Beweisideen ist, a durch x und $\nu_p(x-y)$ durch τ abzuschätzen, so daß die Kongruenz eine Gleichheit wird.

und für $p = 2$

$$\nu_p(a-1) + \nu_p(x+y) = \begin{cases} \tau + \nu_p(\alpha) + \nu_p(z+y'), & \alpha \text{ gerade}, \\ \tau + 1, & \alpha \text{ ungerade}. \end{cases}$$

Für $\nu_p(x-y) > 1$ ist $\nu_p(x+y) = 1 \leqslant \nu_p(z+y')$.

Für $\nu_p(x-y) = 1$ können wir im Fall $x-y = 2$ sagen, daß $x+y = 4$, also $\nu_p(x+y) = 2 \leqslant \nu_p(z+y')$ für $\tau = 1$.

LEMMA 5. *Für eine nichttriviale Lösung von* $(*)$ *mit* (N) *ist*

$$a - 1 \leqslant \begin{cases} x-2 & \text{falls } p > 2,\ \alpha \text{ ungerade}, \\ 3(x-1) & \text{falls } p > 2,\ \alpha \text{ gerade},\ y' = -1, \\ 2(x-1) & \text{falls } p > 2,\ \alpha \text{ gerade},\ y' = 1 \\ & \text{oder } p = 2,\ \nu_p(a-1) \geqslant \tau - 1. \end{cases}$$

Beweis. Wie im Beweis von Lemma 1 gibt es nach (Z) einen ungeraden Primfaktor q von z mit $d_q(x, y) = \alpha \mid q-1$. Wir setzen wieder $q - 1 = \gamma\lambda\alpha$, $z = rq$ mit $\lambda, r \in \boldsymbol{N}$ und

$$\gamma = \begin{cases} 2, & \alpha \text{ ungerade}, \\ 1, & \alpha \text{ gerade}. \end{cases}$$

Dann ist

$$\gamma r\lambda(a-1) = p^\tau x - [r(1+\gamma\lambda) - y'].$$

Aus

$$\nu_p(a-1) \geqslant \begin{cases} \tau, & p \text{ ungerade}, \\ \tau - 1, & p \text{ gerade} \end{cases}$$

folgt

$$\nu_p[\gamma r\lambda(a-1)] \geqslant \tau, \quad \text{also} \quad \nu_p[r(1+\gamma\lambda) - y'] \geqslant \tau.$$

Wir setzen

$$r(1+\gamma\lambda) - y' = \gamma'\varrho p^\tau$$

mit

$$\varrho \in \boldsymbol{N} \quad \text{und} \quad \gamma' = \begin{cases} 2, & p, \alpha \text{ ungerade}, \\ 1, & \text{sonst}. \end{cases}$$

Jetzt ist

$$r(1+\gamma\lambda) - y' \leqslant \gamma'' r\lambda$$

mit

$$\gamma'' = \begin{cases} \gamma + 2, & \lambda = 1,\ y' = -1, \\ \gamma + 1, & \text{sonst}. \end{cases}$$

Nun ist

$$(x - \gamma'\varrho)p^\tau = \gamma r\lambda(a-1) \geqslant \frac{\gamma\gamma'}{\gamma''}\varrho p^\tau(a-1),$$

also
$$\gamma''(x-\gamma') \geqslant \gamma\gamma'(a-1).$$
Daraus ergibt sich die Behauptung.

Aus Lemma 5 werden wir später in Lemma 9 schließen, unter gewissen Voraussetzungen an p muß gelten $\nu_p(a-1) \leqslant \nu_p(x-y)$. Nach Lemma 4 wissen wir, wann $\nu_p(a-1) \geqslant \tau+\nu_p(a)$ ist.

LEMMA 6. *Die einzigen nichttrivialen Lösungen von* (*) *mit* (N) *und* $\nu_p(x-y) \geqslant \tau$ *sind*
$$2^4-1 = 3\cdot 5, \qquad 5+1 = 3\cdot 2,$$
$$3^3+1 = 2^2\cdot 7, \qquad 7-1 = 2\cdot 3,$$
$$7^4-1 = 6\cdot 20^2, \qquad 20+1 = 3\cdot 7.$$

Beweis. Wir setzen $x-y = cp^\sigma$ mit $c, \sigma \in \boldsymbol{N}$ und $(p, c) = 1$. Nach Lemma 3 ist $ap^\tau-yy' = \varkappa x$ mit $\varkappa \in \boldsymbol{N}$,
$$ap^\tau-y(\varkappa+y') = \varkappa(x-y).$$
Nach Voraussetzung ist $\nu_p(\varkappa+y') =: \delta \geqslant \tau$. Wir setzen $\varkappa+y' = wp^\delta$ mit $w, \delta \in \boldsymbol{N}_0$ und $(p, w) = 1$.

Nach Lemma 3 ist für $a > 1$:
$$2y'\varkappa = 2y'(wp^\delta-y') \equiv 1+yy'p^\tau \pmod{x}.$$
Es folgt
$$p^\tau(2wp^{\delta-\tau}-y) \equiv 3y' \pmod{x},$$
$$2wp^{\delta-\tau}-y \equiv -3cyy'p^{\sigma-\tau} \pmod{x}.$$
Es ist
$$x\left(wp^{\delta-\tau}-\frac{y'}{p^\tau}\right) = a-\frac{yy'}{p^\tau} < a+1 \leqslant a.$$
Also

für $y' = -1$ ist $xwp^{\delta-\tau} \leqslant a-1$,

für $y' = 1$ ist $x(wp^{\delta-\tau}-1) \leqslant a-1$.

Mit Lemma 5 schließen wir jetzt für

$p > 2$, a ungerade: Aus $a-1 \leqslant x-2$ folgt $w = 0$ oder $y' = 1$, $w = 1$, $\delta = \tau$.

$p > 2$, a gerade, $y' = -1$: Aus $a-1 \leqslant 3(x-1)$ folgt $wp^{\delta-\tau} < 3$, also $w = 0$ oder $\delta = \tau$, $w = 1, 2$.

$p > 2$, a gerade, $y' = 1$: Aus $a-1 \leqslant 2(x-1)$ folgt $wp^{\delta-\tau}-1 < 2$, also ebenfalls $w = 0$ oder $\delta = \tau$, $w = 1, 2$.

$p = 2$: Nach Lemma 4 ist $\nu_p(a-1) \geqslant \tau$. Aus $a-1 \leqslant 2(x-1)$ folgt $wp^{\delta-\tau} < 2$ für $y' = -1$ und $wp^{\delta-\tau}-1 < 2$ für $y' = 1$, also $w = 0$ oder $\delta = \tau$, $w = 1$ oder $y' = 1$, $w = 1$, $\delta = \tau+1$.

Der Fall $w = 0$ erschließt sich uns aus Lemma 7 und gibt die Lösung $x = 7$, $y = 1$, $a = 4$.

Es sei jetzt $w > 0$.

I. $\delta = \tau$.

Es ist
$$-2wyy' \equiv 3cp^{\sigma-\tau}-y' \pmod{x}.$$
Nun ist $x \geqslant 2w$ ($w = 1$: klar; $w = 2$, $x = 3 \Rightarrow p = 2 \Rightarrow w = 1 \Rightarrow$ W!) außer für $x = 2$, $w = 2$. Dann ist $c = 1$, $p^\sigma = 3$, $y = -1$.

Wir untersuchen, wann die Ungleichung $3cp^{\sigma-\tau}-y' \leqslant x$ gilt. Das ist genau dann der Fall, wenn
$$cp^{\sigma-\tau}(3-p^\tau) \leqslant y+y'.$$
$p^\tau = 2$.

Dann ist $w = 1$ und $2(2-y) \equiv 3y' \pmod{x}$.

$x = c\cdot 2^\sigma+y$ und $4 \equiv 2y+3y' \pmod{x}$ führt auf

$y = 1$, $\quad y' = 1$, $\quad 4 \equiv 5 \pmod{x} \quad \Rightarrow x = 1 \Rightarrow$ W!,

$\qquad y' = -1$, $\quad 4 \equiv -1 \pmod{x} \Rightarrow x = 5$, $\sigma = 2$, $c = 1$,

$y = -1$, $y' = 1$, $\quad 4 \equiv 1 \pmod{x} \quad \Rightarrow x = 3$, $\sigma = 2$, $c = 1$,

$\qquad y' = -1$, $\quad 4 \equiv -5 \pmod{x} \Rightarrow x = 3$, $\sigma = 2$, $c = 1$

oder $x = 9$, $\sigma = 1$, $c = 5$.

Jetzt ist
$$z = 2x+y' = \begin{matrix} 9 \\ 7 \\ 5 \\ 17 \end{matrix} \quad \text{PZ}-\text{Potenz}, \ a \text{ ungerade}.$$
Aus (P_1) folgt a PZ, $z \equiv 1 \pmod{a}$.

Also $z = 7$, $a = 3$. $3^3+1 = 4\cdot 7$ ist Lösung (aber $a = 1$).

$p^\tau = 3$, $y = -1$.

Dann ist $x \equiv -1 \pmod{3}$, $2w+1 \equiv y' \pmod{x}$. Aus $w = 1, 2$ folgt $x = 2$. Nach Lemma 5 ist a gerade, $a-1 \leqslant 3$, d.h. $y' = -1$, $a = 4$. $2^4-1 = 3\cdot 5$ ist Lösung (aber $a = 1$).

Aus Lemma 2 folgt sofort, daß dies die beiden einzigen Lösungen mit $a = 1$ sind.

$p^\tau = 4$, $y = y' = -1$, $c = 1$, $\sigma = \tau$.

Jetzt ist $x = 3$, $z = 11$ PZ. Mit (P_1) folgt a PZ, $z \equiv 1 \pmod{a}$, d.h. $a = 5$. $3^5+1 = 4\cdot 61$, $61 \neq 11^a \Rightarrow$ W!

In allen anderen Fällen ist demnach
$$0 < 2w, \ 3cp^{\sigma-\tau}-y' \leqslant x.$$

Es ist also entweder

$$yy' = 1, \quad x-2w = 3cp^{\sigma-\tau}-y' \quad \text{oder} \quad yy' = -1, \quad 2w = 3cp^{\sigma-\tau}-y'.$$

$yy' = 1$.
Es ist $x = cp^{\sigma}+y$, also

$$cp^{\sigma-\tau}(p^{\tau}-3) = 2(w-y).$$

$w-y = 0 \Rightarrow w = y = 1$, $p^{\tau} = 3$. Diesen Spezialfall behandeln wir in Lemma 8.

$w-y = 1 \Rightarrow w = 2$, $y = 1$. Dann ist p ungerade, a gerade. Also $c = 1$, $\sigma = \tau$, $p^{\tau} = 5$.

Aus $x = 6$, $z = 31$ PZ folgt mit (P_1), daß a PZ, $z \equiv 1 \pmod{a}$. Also $a = 2$. Aber $a \equiv 1 \pmod{p} \Rightarrow$ W!

$w-y = 2 \Rightarrow w = 1$, $y = -1$. Dann ist

$$\begin{array}{llll} p^{\tau}-3 = 1, & p^{\tau} = 4, & c = 1, & p^{\sigma-\tau} = 4, \\ \phantom{p^{\tau}-3 =} 2 & \phantom{p^{\tau} =} 5 & 2 & \sigma = \tau \\ \phantom{p^{\tau}-3 =} 4 & \phantom{p^{\tau} =} 7 & 1 & \sigma = \tau \end{array}$$

also

$$\begin{array}{ll} x = 15, & z = 59 \\ 9 & 44 \\ 6 & 41. \end{array}$$

$x = 6, 15$. Mit (P_1) folgt a PZ, $z \equiv 1 \pmod{a}$. Da $a \equiv 1 \pmod{p}$, ist $x = 15$, $a = 29$ ungerade $\Rightarrow \alpha$ gerade. Andererseits ist $4\alpha-1 = 5x = 75 \Rightarrow \alpha = 19 \Rightarrow$ W!

$x = 9$. Aus $Q(9, -1, a) = Q(9, -1, 2)\,Q(9^2, 1, a/2)$ folgt

$$Q(9^2, 1, a/2) = 2^{2\alpha-3}11^{\alpha}.$$

Dann ist $a/2$ gerade und nach (P_1) PZ, d.h. $a = 4$.

$$9^4-1 = 10\cdot 656 \not\equiv 0 \pmod{11} \Rightarrow \text{W!}$$

$w-y = 3 \Rightarrow w = 2$, $y = -1$. Dann ist p ungerade, a gerade. Also

$$\begin{array}{llll} p^{\tau}-3 = 2, & p^{\tau} = 5, & c = 3, & \sigma = \tau, \\ \phantom{p^{\tau}-3 =} 6 & \phantom{p^{\tau} =} 9 & 1 & \end{array}$$

daher

$$\begin{array}{ll} x = 14, & z = 69 = 3\cdot 23 \\ 8 & 71 \end{array}$$

Da $14 \equiv -1 \pmod{3}$ folgt mit (P_1), daß a PZ, also $a = 2$. Dann ist aber $a \not\equiv 1 \pmod{p} \Rightarrow$ W!

$yy' = -1$.
Ist

$$\begin{array}{lll} y = 1, & \text{so} & w = 2,\ c = 1,\ \sigma = \tau. \\ = -1 & & = 1 \end{array}$$

Ist $w = 2$, so p ungerade, a gerade. Aus $y = 1$, $y' = -1$ folgt α gerade. Andererseits ist $x = p^{\sigma}+y$, gerade, $ap^{\tau} \equiv yy' \pmod{x}$, also α ungerade $\Rightarrow$ W!

Also $w = 1$. Dann ist $y' = 1$, daher α ungerade. Nach Annahme ist $ap^{\tau}+1 = (p^{\tau}-1)x = (p^{\tau}-1)^2 = p^{2\tau}-2p^{\tau}+1 \Rightarrow a = p^{\tau}-2$. Für $p = 2$ ist $\sigma = \tau > 1$. Aus Lemma 4 ergibt sich

$$\nu_p(a-1) \geqslant \tau + \nu_p(\alpha) = \begin{cases} \tau, & p > 2, \\ \tau+1, & p = 2. \end{cases}$$

Aus Größengründen folgt mit Lemma 5 ein Widerspruch.

II. $\delta = \tau+1$.
Dann ist $p = 2$, $y' = 1$, $w = 1$. Wir haben

$$-4y \equiv 3cp^{\sigma-\tau}-1 \pmod{x},$$
$$-3y \equiv 3cp^{\sigma-\tau}-1+y \pmod{x}.$$

Da $x \geqslant 3$, untersuchen wir, wann die Ungleichung

$$3cp^{\sigma-\tau}-1+y \leqslant x = cp^{\sigma}+y$$

gilt. Das ist genau dann der Fall, wenn

$$cp^{\sigma-\tau}(3-p^{\tau}) \leqslant 1$$

ist. Diese Bedingung ist sicherlich erfüllt, wenn $p^{\tau} \geqslant 4$ ist.

$p^{\tau} = 2$.
Aus $2(4-y) \equiv 3 \pmod{x}$ folgt:
für $y = 1$, daß $x = 3$, $z = 7$. Aus (P_1) ergibt sich a PZ, $z \equiv 1 \pmod{a}$ $\Rightarrow a = 3$, $3^3-1 = 2\cdot 13 \not\equiv 0 \pmod{7} \Rightarrow$ W!
für $y = -1$, daß $x = 7$, $z = 15 = 3\cdot 5$. Aus (P_2) ergibt sich $a = s$ oder s^2, s PZ, $3, 5 \equiv 1 \pmod{s} \Rightarrow s = 2 \Rightarrow$ W!

In allen anderen Fällen folgt:

für $y = -1$, daß $3 = 3cp^{\sigma-\tau}-2 \Rightarrow$ W!

für $y = 1$, daß $x-3 = 3cp^{\sigma-\tau}$, $cp^{\sigma-\tau}(p^{\tau}-3) = 2$.

Also $p^{\tau} = 4$, $c = 1$, $\sigma = \tau+1$.
Dann ist $x = 9$, $z = 37$. Nach (P_1) ist a PZ,
$z \equiv 1 \pmod{a} \Rightarrow a = 3$, $9^3-1 = 8\cdot 91 \not\equiv 0 \pmod{37} \Rightarrow$ W!

LEMMA 7. *Die einzige nichttriviale Lösung von* $(*)$ *mit* (N) *und* $ap^{\tau}-$ $-yy' = x$, $\alpha > 1$ *ist*

$$x = 7, \quad y = 1, \quad a = 4.$$

Beweis. Nach Lemma 3 ist $1+yy'p^\tau \equiv 2y' \pmod{x} \Rightarrow p^\tau \equiv y(2-y')$ $(\mathrm{mod}\, x)$. Es ist also

$$p^\tau - y(2-y') = \mu x = \mu(ap^\tau - yy') \quad \text{mit} \quad \mu \in \mathbf{Z}.$$

$\mu < 0$. Dann ist $2 \leqslant p^\tau < y(2-y') \leqslant 3$. Es folgt $p^\tau = 2$, $y(2-y') = 3$, $\mu x = -1 \Rightarrow$ W!

$\mu \geqslant 1$. Dann ist $y\big((\mu+1)y'-2\big) = p^\tau(\mu a-1) > 0$.

$$y' = 1 \Rightarrow y = 1,\ \mu-1 = p^\tau(\mu a-1) > 2\mu-1 \Rightarrow \text{W!}$$

$$y' = -1 \Rightarrow y = -1,\ \mu+3 = p^\tau(\mu a-1) \geqslant 2(2\mu-1) \Rightarrow 3\mu \leqslant 5 \Rightarrow$$
$$\Rightarrow \mu = 1,\ 4 = p^\tau(a-1).$$

Also

$$\begin{array}{llllll} p^\tau = 2, & a = 3, & x = 5, & z = 9, & a \text{ gerade}, \\ \quad\ \ 4 & \quad\ \ 2 & \quad\ \ 7 & \quad\ \ 27 & \quad \text{ungerade}, \end{array}$$

$$5^a-1 = 6\cdot 9^3, \qquad 6\cdot 9^3+1 \equiv -2^3+1 \equiv 0 \pmod 7$$

aber

$$7^a+1 = 8\cdot 27^2,\ 8\cdot 27^2-1 \equiv 8\cdot 7^2-1 \equiv 8\cdot(-2)-1 \equiv 0 \pmod{17} \Rightarrow \text{W!}$$

$\mu = 0$. Dann ist $p^\tau = y(2-y')$. Es folgt $p^\tau = 3$, $y = 1$, $y' = -1$, $x = 3a+1$, $z = 3x-1$.

Beh.: $a = 2 (\Rightarrow x = 7,\ z = 20,\ 7^a-1 = 6\cdot 20^2 \Rightarrow a = 4)$.

Bewies: siehe Lemma 8.

Korollar. *Das Paar diophantischer Gleichungen*

$$p_1^a - y^a = 2^\sigma p_2^\alpha,$$
$$p_2^b - y'^b = 2^\tau p_1^\beta,$$

$a, b, \alpha, \beta, \sigma, \tau \in N$, $\{y, y'\} \subset \{1, -1\}$, p_1, p_2 *Primzahlen, besitzt nur die Lösungen*

$$\begin{array}{lllll} p_1 = 3, \\ a = 3, & y = -1, & p_2 = 7, & y' = 1, & b = 1, 2, \\ & & & y' = -1, & b = 2, \\ & y = 1, & p_2 = 13, & y' = 1, & b = 1, \\ a = 4, & y = 1, -1, & p_2 = 5, & y' = 1, & b = 2, \\ & & & y' = -1, & b = 1, 2, \\ a = 5, & y = 1, & p_2 = 11, & y' = -1, & b = 1. \end{array}$$

Beweis. Wir zerlegen

$$p_1 - y = 2^{\sigma'} p_2^{\alpha'}, \quad \sigma' > 0, \quad Q(p_1, y, a) = 2^{\sigma-\sigma'} p_2^{\alpha-\alpha'},$$
$$p_2 - y' = 2^{\tau'} p_1^{\beta'}, \quad \tau > 0, \quad Q(p_2, y', b) = 2^{\tau-\tau'} p_1^{\beta-\beta'},$$

und betrachten drei Fälle:

A. $\alpha' > 0$, $\beta' > 0$: Es ist

$$p_1+1 \geqslant p_1 - y \geqslant 2p_2,$$
$$p_2+1 \geqslant p_2 - y' \geqslant 2p_1,$$

und es gibt keine Lösungen.

B. $\alpha' = 0$, $\beta' > 0$: Wir zerlegen ferner

$$a = 2^\lambda a' \quad \text{mit} \quad (2, a') = 1,$$
$$p_1^{2^\lambda} - y^{2^\lambda} = 2^\sigma p_2^{\alpha-\tilde\alpha}, \quad Q(p_1^{2^\lambda}, y^{2^\lambda}, a') = p_2^{\tilde\alpha},$$

und betrachten

B_1. $\tilde\alpha = 0$: Nach (P_0) und (P_1) gibt es die Lösungen

$$a' = 1,\ p_1 = 3,\ \lambda = 2,\ p_2 = 5,\ y' = -1,\ b = 1, 2.$$

B_2. $\tilde\alpha > 0$: Nach (P_0) folgt $\tilde\alpha = \alpha$. Aus dem Satz ergeben sich die Lösungen

$$\begin{array}{llllll} p_1 = 3, & \lambda = 0, & y = -1, & a' = 3, & p_2 = 7, & y' = 1, \quad b = 1, 2, \\ & & y = 1, & a' = 3, & p_2 = 13, & y' = 1, \quad b = 1, \\ & & y = 1, & a' = 5, & p_2 = 11, & y' = -1, \quad b = 1. \end{array}$$

C. $\alpha' = 0$, $\beta' = 0$: Wir unterscheiden

C_1. a gerade, b gerade: Aus (P_1) folgt

$$b = 2,\ p_1 = 3,\ a = 4,\ p_2 = 5,\ y' = 1.$$

C_2. a ungerade, b gerade: Dann ist nach (P_1) $b = 2$, und aus dem Satz ergibt sich die einzige Lösung

$$p_1 = 3,\ y = -1,\ a = 3,\ p_2 = 7,\ y' = -1.$$

C_3. a ungerade, b ungerade: Nach (P_1) sind a, b Primzahlen,

$$p_1 \equiv 1 \pmod b, \qquad p_2 \equiv 1 \pmod a.$$

Aus

$$2^\sigma(2^\tau + y')^a = (2^\sigma + y)^a - y^a$$

erhalten wir $\qquad a \equiv \pm 1 \pmod{2^{\min(\sigma,\tau)}}$.

Auf demselben Wege $\qquad b \equiv \pm 1 \pmod{2^{\min(\sigma,\tau)}}$.

Ist $\delta \leqslant \tau$, so

$$p_1 - 1 \geqslant 2b > b+1 \geqslant 2^\sigma \geqslant p_1 - 1,$$

ein Widerspruch.

Dasselbe für $\tau \leqslant \delta$.

Das verallgemeinerte Problem vom Steuerwald

$$p_1^a - y^a = p^\sigma 2^a,$$
$$2^b = y'^b = p^\tau p_1^\beta$$

kann ich nicht vollständig lösen.

Lemma 8. *Es gibt keine nichttrivialen Lösungen von* $(*)$ *mit* (N) *für* $\alpha \geqslant 3$ *und* $p^\tau = 3$, $y = 1$, $\varkappa x = 3\alpha - y'$, $y' = (-1)^\varkappa$, $\varkappa = 1, 2$.

Beweis. Aus $Q(x, y, a-1) = p^\tau Q(z, y', \alpha)$ folgt für $\alpha \geqslant 3$

$$1 + x + x^2 \equiv 3\left[\alpha y' + \binom{\alpha}{2} 3x + \binom{\alpha}{3}(3x)^2 y'\right] \pmod{x^3}$$
$$\equiv 3\alpha y' + \tfrac{1}{2}[(3\alpha)^2 - 3(3\alpha)]x + \tfrac{1}{6}[(3\alpha)^3 - 9(3\alpha)^2 - 18(3\alpha)]x^2 y',$$

also

$$6(1 + x + x^2) \equiv 6(\varkappa x y' + 1) + 3(2\varkappa x y' + 1 - 3\varkappa x - 3y')x +$$
$$+ (1 - 9y' + 18)x^2 \pmod{x^3},$$
$$3 - 6\varkappa y' + 9y' \equiv x(13 + 6\varkappa y' - 9\varkappa - 9y') \pmod{x^2}.$$

$$\varkappa = 2,\ y' = 1 \Rightarrow 0 \equiv -2x \pmod{x^2} \Rightarrow x = 2,\ 4 = 3\alpha - 1 \Rightarrow \text{W!}$$
$$\varkappa = 1,\ y' = -1 \Rightarrow 0 \equiv 7x \pmod{x^2} \Rightarrow x = 7 = 3\alpha + 1 \Rightarrow$$
$$\Rightarrow \alpha = 2 \Rightarrow \text{W!}$$

Lemma 9. *Für eine nichttriviale Lösung von* $(*)$ *mit* (N) *und* $x - y = cp^\sigma$, $c, \sigma \in N$, $(c, p) = 1$ *gilt*

$$\nu_p(a-1) \leqslant \sigma,$$

falls

$$c \leqslant \begin{cases} 2p-1, & p, a \text{ ungerade}, \\ p+1, & p \text{ ungerade}, a \text{ gerade}, \\ 1, & p = 2 \end{cases}$$

und nicht $p = 2$, $x - y = 2$, $a = 5$ *ist*.

Beweis. Angenommen $a - 1 = tp^{\sigma+1}$, $t \in N$. Aus dem Beweis von Lemma 5 erhalten wir

$$\gamma\gamma'\varrho t p \leqslant \gamma'' c.$$

p, a ungerade.

$$\varrho t p \leqslant c \leqslant 2p - 1 \Rightarrow \varrho t = 1 \Rightarrow \text{W!} \quad (t \text{ ist gerade}).$$

p ungerade, a gerade.

Jetzt ist $r > 1$ (sonst folgt mit (P_1), daß $a = 2 \Rightarrow$ W!). Außer für $\lambda = 1$, $y' = -1$ ist

$$\varrho t p \leqslant 2c \leqslant 2(p+1) \Rightarrow \varrho t \leqslant 2.$$

$\varrho = t = 1$. Wegen $(p, r) = 1$ folgt $x \equiv 1 \pmod{r}$. Sei $d > 1$ ein echter Teiler von a. Außer für $d = 2$, $x + y = 2^\nu$ gibt es nach (Z) einen ungeraden Primfaktor q' von z mit $d_{q'}(x, y) = d$. Dann $q' | r \Rightarrow x \equiv 1 \pmod{q'} \Rightarrow y = -1$, $d = 2$. Es ist also immer $d = 2$, d.h. $a = 4 \Rightarrow$ W!

$\varrho = 2$, $t = 1$. Dann ist $c = p + 1$ gerade, x ungerade, z gerade, r gerade. Aus $x \equiv 2 \pmod{r}$ folgt ein Widerspruch. Sei nun $\lambda = 1$, $y' = -1$. Aus

$$rtp^{\sigma+1} = r(a-1) = (x - \varrho)p^\tau = (cp^\sigma + y - \varrho)p^\tau \leqslant cp^{\sigma+\tau}$$

folgt

$$rt \leqslant cp^{\tau-1}.$$

Ist $cp^{\tau-1} > r$, so

$$\varrho p^\tau = 2r + 1 \leqslant 2cp^{\tau-1} - 1, \qquad 1 \leqslant p^{\tau-1}(2c - \varrho p).$$

Dann $\varrho p < 2c \leqslant 2(p+1) \Rightarrow \varrho \leqslant 2 \Rightarrow$ W! (wie oben).

Ist $cp^{\tau-1} = r$, so $t = \tau = 1$, $r = c$, $y = \varrho \Rightarrow \varrho = 1 \Rightarrow$ W! (wie oben).

$p = 2$. Aus $2\varrho t p \leqslant \gamma'' \leqslant 4$ folgt $\varrho = t = 1$, $\lambda = 1$, $y' = -1$. Aus $4(2^\sigma + y - 1) \geqslant 2 \cdot 2^{\sigma+1}$ folgt $y = 1$. Dann ist $r = 1$, $\tau = 2$. Da $\alpha > 1$, ist

$$4a + 1 = \varkappa x, \qquad 2\varkappa \equiv 3 \pmod{x},$$
$$\varkappa x = 4a + 1 \leqslant 8(x-1) + 1 \Rightarrow 7 \leqslant (8 - \varkappa)x \Rightarrow \varkappa \leqslant 7.$$
$$\varkappa = 1 \Rightarrow 2 \equiv 3 \pmod{x} \Rightarrow \text{W!}$$
$$\left.\begin{array}{l} \varkappa = 5 \Rightarrow x = 7 \neq 2^\sigma + 1 \\ \varkappa = 7 \Rightarrow x = 11 \neq 2^\sigma + 1 \end{array}\right\} \Rightarrow \text{W!}$$

Also $\varkappa = 3 \Rightarrow x = 3 \Rightarrow \alpha = 2$, $a = 5$.

Unser Satz ist mit dem folgenden Lemma vollständig bewiesen.

Lemma 10. *Die einzigen nichttrivialen Lösungen von* $(*)$ *mit* (N) *und* $x - y = 2 = p$, a *ungerade oder* $\tau > 1$, a *gerade sind* $x = 3$ *und* $a = 3, 5$.

Beweis. Es ist $x = 3$, $y = 1$. Nach Lemma 4 ist $\nu_p(a-1) = \tau - 1 + \nu_p(\alpha) \geqslant \tau - 1$. Nach Lemma 5 ist $a - 1 \leqslant 4$.

Literatur

[1] K. Inkeri, *On the diophantine equation* $a(x^n-1)/(x-1) = y^m$, Acta Arith. 21 (1972), S. 299–311.

[2] W. Ljunggren, *Noen setninger om ubestemte likninger av formen* $\frac{x^n-1}{x-1} = y^q$, Norske Mat. Tidsskr., 1. Hefte, 25 (1943), S. 17–20.

[3] B. Richter, *Die Primfaktorzerlegung der Werte der Kreisteilungspolynome II*, J. Reine Angew. Math. 267 (1974), S. 77–89.

[4] — *Diophantische Probleme bei Kreisteilungspolynomen*, Diss. FU Berlin, 1975.

[5] T. N. Shorey and R. Tijdeman, *New applications of diophantine approximations to diophantine equations*, Math. Scand. 39 (1976), S. 5–18.

[6] R. Steuerwald, *Ein Satz über natürliche Zahlen N mit $\sigma(N) = 3N$*, Arch. Math. 5 (1954), S. 449–451.
[7] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatshefte f. Math. u. Physik 3 (1892), S. 265–284.

TECHNISCHE UNIVERSITÄT BERLIN
FACHBEREICH 3-MATHEMATIK
D-1000 Berlin 12 (West)

Eingegangen am 26.3.1979
und in revidierter Form am 28.8.1979 (1150)

ACTA ARITHMETICA
XL (1982)

On the class numbers of $Q(\sqrt{\pm 2p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime

by

Pierre Kaplan (Nancy, France) and Kenneth S. Williams* (Ottawa, Canada)

1. Introduction. This paper is a sequel to the paper [4] of the second author and should be read in conjunction with it. For the prime $p = 8l+1$, we consider the ideal class number $h(-2p)$ of $Q(\sqrt{-2p})$ and the ideal class number $h(2p)$ in the narrow sense of $Q(\sqrt{2p})$. It is well known that $h(-2p) \equiv h(2p) \equiv 0 \pmod 4$. Let $\eta_{2p} = R+S\sqrt{2p} > 1$ be the fundamental unit of norm $+1$ of the real quadratic field $Q(\sqrt{2p})$, so that

$$R^2 - 2pS^2 = 1. \tag{1.1}$$

Clearly R is odd and S is even. Our aim is to prove the following theorem.

Theorem.

$$h(-2p) + \frac{S}{2}\cdot h(2p) + p - 1 \equiv 0 \pmod{16}. \tag{1.2}$$

This theorem establishes a conjecture of the first author given in [3], p. 285.

It is known (see for example [1], p. 600) that exactly one of the three equations $x^2-2py^2 = -1, -2, +2$ is solvable in integers x and y. We set $E_p = -1, -2, +2$ accordingly, so that

$$V^2 - 2pW^2 = E_p$$

has rational integral solutions V, W. The following congruences involving $h(2p)$, $h(-2p)$ and $h(-p)$ modulo 8 are known (see for example [1]):

$$h(-2p) \equiv h(-p) + 4l \pmod 8, \tag{1.3}$$

$$h(2p) \equiv 0 \pmod 8 \Leftrightarrow h(-p) \equiv 0 \pmod 8 \text{ and } p \equiv 1 \pmod{16}, \tag{1.4}$$

* Research supported by grant no. A-7233 of the Natural Sciences and Engineering Research Council Canada.