ON A DIOPHANTINE EQUATION OF ANDREJ DUJELLA

K.R. Matthews, J.P. Robertson, J. White

Abstract. We investigate positive solutions (x, y) of the Diophantine equation $x^2 - (k^2 + 1)y^2 = k^2$ that satisfy $y < k - 1$, where $k \geq 2$. It has been conjectured that there is at most one such solution for a given k.

1. Introduction

We consider the diophantine equation

$$x^2 - (k^2 + 1)y^2 = k^2, \tag{1.1}$$

where $k \geq 2$ and $x \geq 1, y \geq 1$.

In 2009, Andrej Dujella remarked that (1.1) always has the solution $(x, y) = (k^2 - k + 1, k - 1)$ and conjectured that there is at most one positive solution (x, y) with $y < k - 1$. We call such a solution an *exceptional* solution. We have verified the conjecture for $k \leq 2^{32}$, with 50374 values of k possessing an exceptional solution. As pointed out by Professor Dujella, the conjecture implies the $D(-1)$ quadruples

2000 *Mathematics Subject Classification.* 11D09.

Key words and phrases. quadratic diophantine equations, continued fractions.

conjecture (see [3]). The conjecture has been proved for $k^2 + 1 = p^n$ or $2p^n$, p an odd prime and when $k = p^{2i+1}$ or $2p^{2i+1}$, (no exceptional solutions) and when $k = 2p^{2i}, p$ an odd prime, where the exceptional solution is $(2p^{3i} + p^i, p^i)$. See [5].

In section 2 we obtain formulae for the exceptional solutions in terms of solutions (p, q) with $\gcd(p, q) = 1$, of the diophantine equation $ap^2 - bq^2 = 2k/d$, where $a > 2, b > 2, \gcd(a, b) = 1$ and $ab = k^2 + 1$. Then p/q is either a convergent to the continued fraction expansion of $\sqrt{b/a}$ if $d > 1$ (which is the case if k is odd), or a near convergent if $d = 1$.

The continued fraction expansion of $\sqrt{b/a}$ has some interesting properties and we state a conjecture which relates the solubility of $ap^2 - bq^2 = 2k$ with $\gcd(p, q) = 1$, to all the partial quotients being even.

In section 8, we introduce the idea of a *Type* 1 exceptional solution (k, x, y), i.e., where $y^2 + 1$ divides either $x + y$ or $x - y$. The Type 1 exceptional solutions where y divides x are easy to describe explicitly, while those where y does not divide x, in fact satisfy $\gcd(x, y) = 1$ and can also be described explicitly.

In section 15, we show that the exceptional solutions form a forest of trees, each arising from a *trivial* solution as root node: those with root node $(t, t, 0), t \geq 2$ are the solutions with $\gcd(x, y) = t$, whereas those with root node $(t, t^2 - t + 1, t - 1), t \geq 2$ or $(t, t^2 + t + 1, t + 1), t \geq 1$ are the ones with $\gcd(x, y) = 1$.

Finally, by studying an extended version of a table of p/q such as Table 1 and using the On–Line Encyclopedia of Integer Sequences

OEIS, we were able to guess some families of exceptional solutions, where a, b, p, q and the continued fraction expansion of $\sqrt{b/a}$ are given explicitly.

2. The parameters d, a, b, p, q

In this section, we derive formulae for the exceptional solution in terms of parameters d, a, b, p, q. The special case of squarefree k was dealt with in [1, §27].

Proposition 2.1. *Suppose* (x, y) *satisfies equation* (1.1). *Let* $d = gcd(x + k, x - k)$ *and define* a, b, p, q *by*

$$a = \gcd((x + k)/d, k^2 + 1), \quad b = \gcd((x - k)/d, k^2 + 1),$$
$$p^2 = (x + k)/da, \quad q^2 = (x - k)/db.$$

Then p *and* q *are integers and*

$$x = d(ap^2 + bq^2)/2, \quad y = dpq$$
$$2k = d(ap^2 - bq^2), \quad \gcd(p, q) = 1$$
$$ab = k^2 + 1, \quad \gcd(a, b) = 1$$
$$k \text{ odd } \implies d \text{ even.}$$

Proof. (i) $x^2 - (k^2+1)y^2 = k^2$ implies $(x+k)(x-k) = (k^2+1)y^2$. Then with $d = gcd(x+k, x-k)$, we have $x+k = du$, $x-k = dv$, where $\gcd(u, v) = 1$. We note that if k is odd, then x is odd and so d is even. Then

$$d^2uv = (k^2 + 1)y^2. \tag{2.1}$$

Let $a = gcd(u, k^2+1), b = gcd(v, k^2+1)$. We prove $ab = k^2+1$. Clearly ab divides $k^2 + 1$, as $\gcd(a, b) = 1$. We have d divides $2k$. If d is odd, then d divides k and $\gcd(d, k^2 + 1) = 1$. If $d = 2D$, then D divides k and $\gcd(D, k^2 + 1) = 1$. Hence if k is even, $\gcd(d, k^2 + 1) = 1$. In both cases, (2.1) implies d divides y and so $k^2 + 1$ divides uv. Finally, assume k is odd. Then $2D^2uv = \frac{(k^2+1)}{2}y^2$, so $y = 2z$. Then

$$D^2uv = (k^2 + 1)z^2$$
$$uv = (k^2 + 1)(z/D)^2$$

and $k^2 + 1$ divides uv. Hence in all cases, $k^2 + 1$ divides the product $\gcd(u, k^2 + 1)\gcd(v, k^2 + 1) = ab$.

Now let $R = u/a, S = v/b$. Then

$$uv = abRS = (k^2 + 1)RS$$
$$d^2uv = d^2(k^2 + 1)RS = (k^2 + 1)y^2.$$

Hence $d^2RS = y^2$, so $y = dY$ and $RS = Y^2$. Hence as $\gcd(R, S) = 1$, we have $R = p^2, S = q^2, Y = pq$ and $y = dpq$. We note that $\gcd(ap^2, bq^2) = \gcd(aR, bS) = \gcd(u, v) = 1$. Also

$2x = d(u+v) = d(ap^2 + bq^2)$ and $2k = d(u-v) = d(ap^2 - bq^2)$. □

3. Some properties of exceptional solutions

Lemma 3.1. *If* (x, y) *is an exceptional solution of* (1.1)*, then* $a > 2$ *and* $b > 2$*. Also* $d \neq k$ *and* $d \neq 2k$*.*

Proof. (i) First note that $d = k$ or $2k$ would imply k divides $x+k$ and hence k divides x. This in turn implies k divides y, contradicting $y < k - 1$.

(ii) Suppose $a = 1$. Then $b = k^2 + 1$ and $p^2 - (k^2 + 1)q^2 = 2k/d$. Then $p^2 > (k^2 + 1)q^2 > k^2$, so $p > k$ and $y = dpq = pq > k$, which is a contradiction.

(iii) Suppose $b = 1$, Then $a = k^2 + 1$ and $(k^2 + 1)p^2 - q^2 = 2k/d$. Then $q^2 = (k^2 + 1)p^2 - 2k/d \geq k^2 + 1 - 2k = (k - 1)^2$, so $q \geq k - 1$ and $y = dpq \geq k - 1$, which is a contradiction.

The cases $a = 2$ and $b = 2$ are dealt with similarly. □

LEMMA 3.2. *For an exceptional solution, p and q satisfy the following inequalities:*

$$p^2 < (k^2 + 1)/da, \quad q^2 < (k - 1)^2/db. \tag{3.1}$$

PROOF. If (k, x, y) is an exceptional solution, then $y < k - 1$, so $x < k^2 - k + 1$. Hence

$$p^2 = (x + k)/da < (k^2 + 1)/da$$
$$q^2 = (x - k)/db < (k - 1)^2/db.$$

□

4. EXCEPTIONAL y ARE SMALL

PROPOSITION 4.1. *If (x, y) is an exceptional solution of (1.1), then*

$$y \leq 2k - \sqrt{3k^2 + 4}. \tag{4.1}$$

Hence $y < (2 - \sqrt{3})k < 0.268k$.

PROOF. Equation (1.1) gives

$$x^2 = k^2y^2 + k^2 + y^2 = (ky + 1)^2 + (k - y)^2 - 1.$$

From $y < k-1$, we have $k-y > 1$ and so $x > ky+1$. This gives

$$(ky+1)^2 + (k-y)^2 - 1 \geq (ky+2)^2$$

or

$$y^2 - 4ky + k^2 - 4 \geq 0.$$

The polynomial $f(y) = y^2 - 4ky + k^2 - 4$ has roots $y = 2k \pm \sqrt{3k^2+4}$. To have $f(y) \geq 0$ and $0 < y < k-1$, we must have

$$y \leq 2k - \sqrt{3k^2+4}.$$

As $\sqrt{3k^2+4} > k\sqrt{3}$, we have $y < (2-\sqrt{3})k$. □

The example $k = 30$ with exceptional solution $x = 242, y = 8$, shows that inequality (4.1) is sharp. For $3k^2 + 4 = 2704 = 52^2$ and $y = 2k - \sqrt{3k^2+4}$.

5. Connections with continued fractions

LEMMA 5.1. *Consider the equation*

$$ap^2 - bq^2 = 2k/d,$$

where a, b, k, p, q *are positive,* $D = ab = k^2+1, \gcd(a,b) = 1 = \gcd(p,q)$ *and* d *is even if* k *is odd. Let* $(P_m + \sqrt{D})/Q_m$ *denote the* m*–th complete quotient in the continued fraction expansion of* $\sqrt{D}/a = \sqrt{b/a}$.

(i) *If* $d \geq 2$*, then* $p/q = A_m/B_m$*, a convergent of* $\sqrt{b/a}$*. Also*

$$Q_{m+1} = 2k/d, \tag{5.1}$$

where m *is odd.*

(ii) *If* $d = 1$, *then* $p/q = (A_m + eA_{m-1})/(B_m + eB_{m-1})$, *where* $e = \pm 1$. *Also*

$$(-1)^m(Q_m - Q_{m+1} + 2eP_{m+1}) = 2k. \tag{5.2}$$

Proof.

$$ap^2 - bq^2 = 2k/d \implies p\sqrt{a} - q\sqrt{b} = \frac{2k}{d(p\sqrt{a} + q\sqrt{b})}$$
$$\implies p/q - \sqrt{b/a} = \frac{2k}{d(p\sqrt{a} + q\sqrt{b})q\sqrt{a}}.$$

Then

$$0 < p/q - \sqrt{b/a} < \frac{2k}{d(2q\sqrt{b})q\sqrt{a}} = \frac{2k}{2dq^2\sqrt{k^2+1}} < \frac{1}{dq^2}. \tag{5.3}$$

Hence if $d \geq 2$, we have $|p/q - \sqrt{b/a}| < 1/2q^2$ and hence $p/q = A_m/B_m$, a convergent to $\sqrt{b/a}$. Also

$$aA_m^2 - bB_m^2 = (-1)^{m+1}Q_{m+1} = 2k/d,$$

so $Q_{m+1} = 2k/d$ and m is odd.
If $d = 1$, inequality (5.3) gives $|p/q - \sqrt{b/a}| < 1/q^2$ and hence by the Worley–Dujella lemma [2], we have

$$p/q = (A_m + eA_{m-1})/(B_m + eB_{m-1}),$$

where $e = 0$ or ± 1 and $m \geq 0$. If $e = 0$, then $Q_{m+1} = 2k$. Now $(P_{m+1} + \sqrt{D})/Q_{m+1}$ is reduced, so

$$(P_{m+1} + \sqrt{D})/Q_{m+1} > 1 \text{ and } -1 < (P_{m+1} - \sqrt{D})/Q_{m+1} < 0.$$

Hence $\sqrt{D} > P_{m+1} > 2k - \sqrt{D} > k - 1$, which implies $P_{m+1} = k$. However $D - P_{m+1}^2 \equiv 0 \pmod{Q_{m+1}}$, i.e., $k^2 + 1 - k^2 \equiv 0 \pmod{2k}$, giving the contradiction $1 \equiv 0 \pmod{2k}$.

Finally,

$$2k = ap^2 - bq^2 = a(A_m + eA_{m-1})^2 - b(B_m + eB_{m-1})^2$$
$$= (-1)^m(Q_m - Q_{m+1} + 2eP_{m+1}). \tag{5.4}$$

(See [4, Lemma 2].) □

REMARK 5.2. In case (ii) all Q_i appear to be odd. This is equivalent to the P_i being even, by the identity $Q_iQ_{i-1} = D - P_i^2$ ([7, p. 69]) and the fact that k is even here, so that D is odd. The evenness of the P_i is further equivalent to all partial quotients a_i being even, by the identity $P_{i+1} = a_iQ_i - P_i$ ([7, p. 70]).

REMARK 5.3. If $ap^2 - bq^2 = 2k/d$ has a solution with $\gcd(p, q) = 1$, then $bp_1^2 - aq_1^2 = 2k/d$ has a solution $(p_1, q_1) = (kp - bq, ap - kq)$ with $\gcd(p_1, q_1) = 1$. So computationally, it suffices to consider the continued fraction of $\sqrt{b/a}$ where $a < b$.

Table 1 lists the $(k, a, b, d, p/q)$ corresponding to exceptional solutions for $k \leq 1000$.

6. On the continued fraction expansion of $\sqrt{b/a}$

LEMMA 6.1. ([7, p. 81]) *Suppose Q_0 divides D and $\sqrt{D}/Q_0 > 1$. Then*

$$\sqrt{D}/Q_0 = [a_0, \overline{a_1, \ldots, a_{l-1}, 2a_0}],$$

with palindromic symmetries for the three sequences

$$a_1, a_2, \ldots, a_{l-2}, a_{l-1},$$

$$P_1, P_2, \ldots, P_{l-1}, P_l,$$

$$Q_0, Q_1, \ldots, Q_{l-1}, Q_l.$$

k	x	y	a	b	d	p/q	Type
8	18	2	13	5	2	$A_1/B_1 = 1/1$	1
12	17	1	29	5	1	$(A_1 - A_0)/(B_1 - B_0) = 1/1$	1
18	57	3	25	13	3	$A_1/B_1 = 1/1$	1
21	47	2	34	13	2	$A_1/B_1 = 1/1$	1
30	242	8	17	53	4	$A_1/B_1 = 2/1$	2
32	132	4	41	25	4	$A_1/B_1 = 1/1$	1
50	255	5	61	41	5	$A_1/B_1 = 1/1$	1
55	123	2	89	34	2	$A_1/B_1 = 1/1$	1
70	99	1	169	29	1	$(A_1 - A_0)/(B_1 - B_0) = 1/1$	1
72	438	6	85	61	6	$A_1/B_1 = 1/1$	1
80	253	3	37	173	1	$(A_0 + A_{-1})/(B_0 + B_{-1}) = 3/1$	1
98	693	7	113	85	7	$A_1/B_1 = 1/1$	1
105	1893	18	37	298	6	$A_1/B_1 = 3/1$	2
112	3362	30	193	65	2	$A_3/B_3 = 3/5$	2
119	1433	12	194	73	2	$A_3/B_3 = 2/3$	2
128	1032	8	145	113	8	$A_1/B_1 = 1/1$	1
144	322	2	233	89	2	$A_1/B_1 = 1/1$	1
154	487	3	641	37	1	$(A_1 - A_0)/(B_1 - B_0) = 1/3$	1
162	1467	9	181	145	9	$A_1/B_1 = 1/1$	1
200	2010	10	221	181	10	$A_1/B_1 = 1/1$	1
203	837	4	130	317	2	$A_1/B_1 = 2/1$	1
208	4373	21	509	85	1	$(A_2 + A_1)/(B_2 + B_1) = 3/7$	2
242	2673	11	265	221	11	$A_1/B_1 = 1/1$	1
252	8068	32	65	977	8	$A_1/B_1 = 4/1$	2
288	3468	12	313	265	12	$A_1/B_1 = 1/1$	1
333	1373	4	853	130	2	$A_1/B_1 = 1/2$	1
338	4407	13	365	313	13	$A_1/B_1 = 1/1$	1
377	843	2	610	233	2	$A_1/B_1 = 1/1$	1
392	5502	14	421	365	14	$A_1/B_1 = 1/1$	1
408	577	1	985	169	1	$(A_1 - A_0)/(B_1 - B_0) = 1/1$	1
414	2111	5	101	1697	1	$(A_0 + A_{-1})/(B_0 + B_{-1}) = 5/1$	1
418	46818	112	241	725	4	$A_3/B_3 = 7/4$	2
450	6765	15	481	421	15	$A_1/B_1 = 1/1$	1
495	24755	50	101	2426	10	$A_1/B_1 = 5/1$	2
512	8208	16	545	481	16	$A_1/B_1 = 1/1$	1
546	4402	8	1237	241	4	$A_1/B_1 = 1/2$	2
578	9843	17	613	545	17	$A_1/B_1 = 1/1$	1
612	64263	105	865	433	3	$A_3/B_3 = 5/7$	2
616	3141	5	3757	101	1	$(A_1 - A_0)/(B_1 - B_0) = 1/5$	1
648	11682	18	685	613	18	$A_1/B_1 = 1/1$	1
684	2163	3	949	493	3	$A_1/B_1 = 1/1$	1
697	8393	12	505	962	2	$A_1/B_1 = 3/2$	2
722	13737	19	761	685	19	$A_1/B_1 = 1/1$	1
737	4483	6	290	1873	2	$A_1/B_1 = 3/1$	1
800	16020	20	841	761	20	$A_1/B_1 = 1/1$	1
858	61782	72	145	5077	12	$A_1/B_1 = 6/1$	2
882	18543	21	925	841	21	$A_1/B_1 = 1/1$	1
968	21318	22	1013	925	22	$A_1/B_1 = 1/1$	1
987	2207	2	1597	610	2	$A_1/B_1 = 1/1$	1

TABLE 1. Exceptional solutions $(k, x, y), k \leq 1000$.

LEMMA 6.2. *Let* $\sqrt{b/a} = [a_0, \overline{a_1, \ldots, a_{l-1}, 2a_0}]$, *where* $b > a$ *and* $\gcd(a, b) = 1$. *Then*

$$bB_{l-1} = a(a_0 A_{l-1} + A_{l-2}) \tag{6.1}$$

$$A_{l-1} = a_0 B_{l-1} + B_{l-2}. \tag{6.2}$$

In particular, a *divides* B_{l-1}.

PROOF.

$$\begin{aligned}\sqrt{b/a} &= [a_0, \ldots, a_{l-1}, 2a_0 + (\sqrt{b/a} - a_0)]\\ &= [a_0, \ldots, a_{l-1}, a_0 + \sqrt{b/a}]\\ &= \frac{A_{l-1}(a_0 + \sqrt{b/a}) + A_{l-2}}{B_{l-1}(a_0 + \sqrt{b/a}) + B_{l-2}}.\end{aligned}$$

The desired result then follows by cross-multiplying and equating corresponding coefficients. ∎

LEMMA 6.3. *Suppose* $1 < a < b, \gcd(a, b) = 1, ab = k^2 + 1, D = ab$. *Then*

(i) *The period–length* l *of* $\sqrt{b/a}$ *is odd.*
(ii) $A_{l-1}/B_{l-1} = k/a$.
(iii) $A_{l-2}/B_{l-2} = (b - ka_0)/(k - aa_0)$.
(iv) $A_l/B_l = (b + ka_0)/(k + aa_0)$.

PROOF. Let $(x, y) = (k, a)$. Then $\gcd(k, a) = 1$ and

$$ax^2 - by^2 = a(k^2 - ab) = a(k^2 - (k^2 + 1)) = -a.$$

A standard argument shows that x/y is a convergent $k/a = A_{t-1}/B_{t-1}$ of $\sqrt{b/a}$. Then $aA_{t-1}^2 - bB_{t-1}^2 = (-1)^t Q_t = -a$, $Q_t = a$ and t is odd.

Then $DB_{t-1} = (A_{t-1}P_t + A_{t-2}Q_t)Q_0$ by [7, p. 70]. This gives

$$(ab)a = (kP_t + A_{t-2}a)a$$

$$ab = kP_t + A_{t-2}a. \tag{6.3}$$

Hence a divides kP_t and so a divides P_t. Suppose $P_t = aP$. Then as $\xi_t = (P_t+\sqrt{D})/Q_t = P+(\sqrt{D})/a$ is reduced, we have $P = \lfloor(\sqrt{D})/a\rfloor = a_0$. So $\xi_t = a_0 + \xi_0$ and we have found a period for $(\sqrt{D})/a$ of length t. Let l be the least period–length. Then $l \leq t$. Also by Lemma 6.2, $a = B_{t-1}$ divides B_{l-1} and so $t \leq l$. Consequently $l = t$ and hence l is odd.

Next, from (6.3), we have $b = ka_0 + A_{t-2}$, so $A_{t-2} = b - ka_0$. Also from [7, p.70], $P_tB_{t-1} = A_{t-1}Q_0 - Q_tB_{t-2}$, so

$$P_ta = ka - aB_{t-2}$$

$$P_t = aa_0 = k - B_{t-2}$$

and hence $B_{t-2} = k - aa_0$. Finally,

$$A_l = a_lA_{l-1} + A_{l-2} = 2a_0k + (b - ka_0) = b + ka_0$$

$$B_l = a_lB_{l-1} + B_{l-2} = 2a_0a + (k - aa_0) = k + aa_0.$$

□

The next result narrows down the search for p and q, which correspond to an exceptional solution.

Corollary 6.4. *Let l be the period length of the continued fraction expansion for $\sqrt{b/a}$, where $ab = k^2 + 1, \gcd(a, b) = 1$ and $1 < a < b$.*

(i) *If $d > 1$, then $p/q = A_m/B_m$, where $m \leq l - 2$.*

(ii) *If* $d = 1$*, then* $p/q = (A_m + eA_{m-1})/(B_m + eB_{m-1}), e = \pm 1$*, where* $m \leq l - 1$*.*

Proof. From Lemma 3.2, we have $p^2 < (k^2 + 1)/2d$.

(i) If $d > 1$, we know from Lemma 5.1 that $p/q = A_m/B_m$ and $p^2 < (k^2 + 1)/4 < k^2$. Hence $A_m = p < k = A_{l-1}$ and so $m < l - 1$.

(ii) If $d = 1$, Lemma 5.1 implies $p/q = (A_m - eA_{m-1})/(B_m - eB_{m-1})$. If $e = 1$, then $p = A_m + A_{m-1} < A_{l-1}$ and so $A_m < A_{l-1}$, as before. If $e = -1$, then $p = A_m - A_{m-1} \geq A_{m-2}$, and $m - 2 < l - 1$. Hence $m \leq l$. But $m = l$ implies $p = A_m - A_{m-1} = A_l - A_{l-1} = 2ka_0$, which contradicts the inequality $p^2 < (k^2 + 1)/2$. Hence $m \leq l - 1$. □

7. Experimental results for $ap^2 - bq^2 = 2k/d, \gcd(p, q) = 1$

Consider the family of equations $ap^2 - bq^2 = \pm 2k/d$, where d divides $2k$ (with d even if k is odd), $\gcd(a, b) = 1, D = ab = k^2 + 1, 2 < a < b$.

(i) Then there is at most one (a, b, d) for which solubility occurs with $\gcd(p, q) = 1$.

(ii) Let (p_0, q_0) and (p_1, q_1) be the least and second least positive solutions. Then $dp_0q_0 < k - 1 < dp_1q_1$.

(iii) Let $ap_0^2 - bq_0^2 = N$. Then there are two classes of primitive solutions for $ap^2 - bq^2 = N$ with fundamental solutions $(\pm p_0, q_0)$. Also there are two classes of primitive solutions for $ap^2 - bq^2 = -N$ with fundamental solutions $(\pm p_1, q_1)$.

Example 7.1. (i) $k = 8$. Then $k^2 + 1 = 65$ and only $(a, b, d) = (5, 13, 2)$ give solubility of $ap^2 - bq^2 = \pm 2k/d$ with $\gcd(p, q) = 1$ and $2 < a < b, ab = 65, \gcd(a, b) = 1$.

$$\sqrt{13/5} = (0 + \sqrt{65})/5 = [1, \overline{1, 1, 1, 1, 2}].$$

m	a_m	$(P_m+\sqrt{D})/Q_m$	A_m/B_m
0	1	$(0+\sqrt{65})/5$	$1/1$
1	1	$(5+\sqrt{65})/8$	$2/1$
2	1	$(3+\sqrt{65})/7$	$3/2$
3	1	$(4+\sqrt{65})/7$	$5/3$
4	1	$(3+\sqrt{65})/8$	$8/5$
5	2	$(5+\sqrt{65})/5$	$21/13$

From the first period

$$5A_0^2 - 13B_0^2 = (-1)^1 Q_1 = -8$$

$$5A_3^2 - 13B_3^2 = (-1)^4 Q_4 = 8.$$

Then $(p_0, q_0) = (A_0, B_0) = (1, 1)$ is the smallest primitive solution of $5p^2 - 13q^2 = -8$, while $(p_1, q_1) = (A_3, B_3) = (5, 3)$ is the smallest primitive solution of $5p^2 - 13q^2 = 8$. Also (p_0, q_0) gives the exceptional solution $(x_0, y_0) = (18, 2)$ of $x^2 - 65y^2 = 64$.

(ii) $k = 12$. Here $D = k^2+1 = 145$ and only $(a, b, d) = (5, 29, 1)$ give solubility of $ap^2 - bq^2 = \pm 2k/d$ with $\gcd(p, q) = 1$ and $2 < a < b$, $ab = 145$, $\gcd(a, b) = 1$.

$$\sqrt{29/5} = (0+\sqrt{145})/5 = [2, \overline{2, 2, 4}].$$

m	a_m	$(P_m+\sqrt{D})/Q_m$	A_m/B_m
0	2	$(0+\sqrt{145})/5$	$2/1$
1	2	$(10+\sqrt{145})/9$	$5/2$
2	2	$(8+\sqrt{145})/9$	$12/5$
3	4	$(10+\sqrt{145})/5$	$53/22$

From the first period we read off

$$5(A_0 - A_{-1})^2 - 29(B_0 - B_{-1})^2 = (-1)^0(Q_0 - Q_1 - 2P_1) = -24$$
$$5(A_2 + A_1)^2 - 29(B_2 + B_1)^2 = (-1)^2(Q_2 - Q_3 + 2P_3) = 24.$$

Then $(p_0, q_0) = (A_0 - A_{-1}, B_0 - B_{-1}) = (1, 1)$ is the smallest primitive solution of $5p^2 - 29q^2 = -24$, while $(p_1, q_1) = (A_2 + A_1, B_2 + B_1) = (17, 7)$ is the smallest primitive solution of $5p^2 - 29q^2 = 24$. Also (p_0, q_0) gives the exceptional solution $(x_0, y_0) = (17, 1)$ of $x^2 - 145y^2 = 144$.

8. Type 1 and Type 2 exceptional solutions

We can rewrite equation (1.1) as

$$x^2 - y^2 = (y^2 + 1)k^2. \tag{8.1}$$

Definition 8.1. *If (x, y) is an exceptional solution of (1.1) such that*

$$x \equiv \epsilon y \pmod{y^2 + 1}, \tag{8.2}$$

where $\epsilon = \pm 1$, we call (x, y) a Type 1 solution of (1.1). Any other exceptional solution is called a Type 2 solution.

In the range $2 \leq k \leq 1000$, there are 37 Type 1 and 12 Type 2 exceptional solutions (see Table 1) while in the range $2 \leq k \leq 2^{32}$, there are 48717 Type 1 and 1657 Type 2 exceptional solutions.

9. Exceptional solutions where y divides x.

It is easy to derive formulae for k and x in terms of y, when y divides x.

THEOREM 9.1. *Suppose* (x, y) *is an exceptional solution of* (1.1) *such that* y *divides* x. *Then*

$$x + k\sqrt{y^2+1} = y(2y^2 + 1 + 2y\sqrt{y^2+1})^n, \tag{9.1}$$

where $ny > 1$. *Conversely if* k, x, y *satisfy* (9.1) *where* $ny > 1$, *then* (x, y) *is an exceptional solution of* (1.1) *with* y *dividing* x.

PROOF. If (x, y) is a solution of (1.1) such that y divides x, then we see y^2 divides k^2 and hence y divides k. From (1.1) we have

$$(x/y)^2 - (y^2+1)(k/y)^2 = 1. \tag{9.2}$$

This is a Pell equation whose positive solutions $(x/y, k/y)$ are given by

$$(x/y) + (k/y)\sqrt{y^2+1} = (2y^2 + 1 + 2y\sqrt{y^2+1})^n, n \geq 1.$$

Hence

$$x + k\sqrt{y^2+1} = y(2y^2 + 1 + 2y\sqrt{y^2+1})^n. \tag{9.3}$$

Suppose $n = 1$. Then $k = 2y^2 > y + 1$ and hence $y > 1$. Consequently $ny > 1$.

Conversely, assume k, x, y satisfy (9.3), where $ny > 1$. Then

$$x - k\sqrt{y^2+1} = y(2y^2 + 1 - 2y\sqrt{y^2+1})^n. \tag{9.4}$$

Multiplying corresponding sides of (9.3) and (9.4) gives

$$x^2 - k^2(y^2+1) = y^2((2y^2+1)^2 - (2y)^2(y^2+1) = y^2,$$

so (x, y) satisfies (1.1). Also the formula

$$x = y \sum_{i=0, i \text{ even}}^{n} \binom{n}{i} (2y^2+1)^{n-i}(2y)^i(y^2+1)^{i/2} \tag{9.5}$$

reveals that y divides x. Hence y divides k and $y \leq k$. But we cannot have $y = k$ as this gives $x^2 = k^4 + 2k^2$ and so $(k^2+1)^2 - x^2 = 1$. Hence $(k^2 + 1 + x)(k^2 + 1 - x) = 1$, which clearly gives a contradiction. Also $y = k - 1$ implies $k - 1$ divides k, so $k = 2, y = 1, x = 3$. Then (9.3) becomes

$$3 + 2\sqrt{5} = (3 + 2\sqrt{5})^n,$$

which implies $n = 1$ and hence $ny = 1$. □

EXAMPLE 9.2. (a) $n = 1, y > 1$ gives $x = 2y^3 + y$ and $k = 2y^2$, an example in [5], where it was proved that the exceptional solution (x, y) is unique if y is a prime.
(b) $n = 2$ gives $x = 8y^5 + 8y^3 + y$ and $k = 8y^4 + 4y^2$.

THEOREM 9.3. *The solutions* (x, y) *given by* (9.1) *are of Type* 1.

PROOF. If $y = 1$, (9.2) gives $x^2 - 2k^2 = 1$ and x is odd. Hence $x - 1$ is divisible by $y^2 + 1$ and so (x, y) is a Type 1 exceptional solution.

If $y > 1$, on considering (9.5) $\pmod{y^2+1}$, only the term $i = 0$ remains and we get

$$x \equiv (-1)^n y \pmod{y^2 + 1},$$

showing that (x, y) is a Type 1 solution. □

10. THE STRUCTURE OF TYPE 1 EXCEPTIONAL SOLUTIONS

In this section, we prove that if (x, y) is a Type 1 solution for which y does not divide x, then $\gcd(x, y) = 1$.

LEMMA 10.1. *There is a 1–1 correspondence between the Type* 1 *solutions* $(x, y), x \equiv \epsilon y \pmod{y^2+1}, \epsilon = \pm 1$ *and integer pairs* (r, s) *which satisfy* $1 < r < s$ *and*

$$r^2 + s^2 = k^2 + 1 \tag{10.1}$$

$$s \equiv \epsilon \pmod{r}, \tag{10.2}$$

given by

$$r = \frac{x - \epsilon y}{y^2 + 1}, \quad s = \frac{xy + \epsilon}{y^2 + 1}, \tag{10.3}$$

where we take $\epsilon = 1$ *if* $y = 1$*. The inverse is given by the equations*

$$x = r + ys \tag{10.4}$$

$$s = yr + \epsilon. \tag{10.5}$$

PROOF. Assume (x, y) is a Type 1 solution and that (r, s) is given by (10.3). Then

(i)

$$\begin{aligned} r^2 + s^2 &= \frac{(x^2 - 2xy\epsilon + y^2) + (x^2y^2 + 2xy\epsilon + 1)}{(y^2+1)^2} \\ &= \frac{x^2(y^2+1) + y^2 + 1}{(y^2+1)^2} = \frac{x^2+1}{y^2+1} = k^2 + 1. \end{aligned}$$

(ii)

$$r + ys = \frac{x - \epsilon y + y(xy + \epsilon)}{y^2 + 1} = \frac{x(y^2+1)}{y^2+1} = x.$$

(iii)

$$yr + \epsilon = \frac{y(x - \epsilon y) + \epsilon(y^2 + 1)}{y^2 + 1} = \frac{xy + \epsilon}{y^2 + 1} = s.$$

Hence $s \equiv \epsilon \pmod{r}$.

(iv) $x^2 = (k^2+1)y^2 + k^2 > y^2$, so $x > y$. Hence $r > 0$ and so $r \geq 1$. But $r = 1$ implies $y^2 + 1 = x - \epsilon y$, $x = \epsilon y + y^2 + 1$ and (1.1) implies

$$(\epsilon y + y^2 + 1)^2 - (y^2+1)k^2 = y^2$$
$$y^2 + 2\epsilon y + 1 - k^2 = 0,$$

giving $y = -\epsilon + k$. However this contradicts $y < k - 1$. Hence $r > 1$.

(v) We have the equivalence

$$r < s \iff x - \epsilon y < xy + \epsilon \iff -\epsilon(y+1) < x(y-1). \tag{10.6}$$

Case 1. Assume $y > 1$. Then

$$x^2 = k^2y^2 + y^2 + k^2 > y^2 + 2y + 1 = (y+1)^2,$$

so $x > y+1$. Hence $x(y-1) > (y+1)(y-1) \geq y+1$ and (10.6) implies $r < s$.

Case 2. Assume $y = 1$. Then $r = (x-1)/2 < (x+1)/2 = s$.

Conversely, assume $r^2 + s^2 = k^2 + 1$, where $s \equiv \epsilon \pmod{r}$ and $1 < r < s$. With y defined by $s = yr + \epsilon$ and $x = r + ys$, we have

$$\begin{aligned} x^2 - (k^2+1)y^2 &= (r+ys)^2 - (r^2+s^2)y^2 \\ &= r^2 + 2sry - r^2y^2 \\ &= r^2 + 2s(s-\epsilon) - (s-\epsilon)^2 \\ &= r^2 + s^2 - 1 = k^2. \end{aligned}$$

Also $x - y\epsilon = (r+ys) - y\epsilon = r + y^2r = r(1+y^2)$ and it follows that (x, y) is a Type 1 solution to (1.1).

Finally we have to prove $y < k-1$, or $(s-\epsilon)/r < k-1$. We have $s < k$. Hence $s - \epsilon \le k$ and $(s-\epsilon)/r \le k/2 < k-1$.

□

LEMMA 10.2. *Assume* (x, y) *is a Type* 1 *solution with* $\gcd(x, y) = 1$. *Then* x *is odd.*

(i) *If* y *is even, then* $r = u^2$, *where* u *is odd and* $k = uv$, *where* $\gcd(u, v) = 1$.

(ii) *If* y *is odd and* $x + \epsilon y \equiv 0 \pmod 4$, *then* $r = u^2$, *where* u *is odd,* $k = uv$, v *is even and* $\gcd(u, v) = 1$.

(iii) *If* y *is odd and* $x + \epsilon y \equiv 2 \pmod 4$, *then* $r = 2u^2$, *where* u *is odd,* $k = uv$, v *is even and* $\gcd(u, v) = 1$.

PROOF. Assume (x, y) satisfies $\gcd(x, y) = 1$ and is a Type 1 exceptional solution. If y is even, then x is odd. Also if y is odd, the equation $x^2 = y^2 + (y^2 + 1)k^2$ shows x is odd.

Now let $d = \gcd(x - y, x + y)$. Then $d = 1$ if y is even, while $d = 2$ if y is odd.

We have

$$\left(\frac{x - \epsilon y}{y^2 + 1}\right)(x + \epsilon y) = k^2. \tag{10.7}$$

(i) Assume y is even. Then (10.7) gives $r = u^2$, $x + \epsilon y = v^2$, where $\gcd(u, v) = 1$ and $k = uv$.

Assume y is odd. Then $x - \epsilon y = 2X, x + \epsilon y = 2Y$, with $\gcd(X, Y) = 1$. Then

$$\left(\frac{X}{(y^2 + 1)/2}\right)(2Y) = k^2$$

and $k = 2K$ say. Hence

$$\left(\frac{X}{(y^2+1)/2}\right) Y = 2K^2.$$

(ii) Assume $x + \epsilon y \equiv 0 \pmod 4$. Then Y is even, $Y = 2V^2$, X is odd and $r = X/((y^2+1)/2) = u^2$, where u is odd, $k = 2uV = uv$, where v is even and $\gcd(u, v) = 1$.
(iii) Assume $x + \epsilon y \equiv 2 \pmod 4$. Then Y is odd, $Y = V^2$, $X/2$ is odd and

$$r/2 = (X/2)/((y^2+1)/2) = u^2,$$

where u is odd. Then $r = 2u^2$, $k = 2uV = uv$, where u is odd, v is even and $\gcd(u, v) = 1$. $\square$

11. Type 1 solutions (x, y) have $gcd(x, y) = y$ or 1.

Lemma 11.1. *With r defined as in Lemma 10.1, let $h = k - ry$. Then $r > h \geq 0$.*

Proof.

$$\begin{aligned} r > h &\iff r > k - ry \\ &\iff r(y+1) > k \\ &\iff r^2(y^2 + 2y + 1) > k^2 = r^2 + s^2 - 1 = r^2 + (yr + \epsilon)^2 - 1 \\ &\iff 2ry(r - \epsilon) > 0. \end{aligned}$$

However $r - \epsilon \geq 1$ and consequently $r > h$.
Also $ry + \epsilon = s \leq k - 1$, so $0 \leq 1 + \epsilon \leq k - ry = h$. $\square$

Theorem 11.2. *For a Type 1 solution (x, y) of (1.1), either y divides x or* $\gcd(x, y) = 1$.

Proof. We present the proof in the form of an algorithm. First we note that from $x = r + ys$, we have $\gcd(x, y) = \gcd(r, y)$.

Let $r_0 = r, h_0 = h$. From $r^2 + s^2 = k^2 + 1$, substituting $s = ry + \epsilon$ and $k = ry + h$ gives

$$r_0^2 - 2r_0 y(h_0 - \epsilon) - h_0^2 = 0. \tag{11.1}$$

Hence $h_0 = 0$ implies $r_0(r_0 + 2y\epsilon) = 0$ and so $r_0 = -2y\epsilon$ and y divides r_0 and hence x. Also equation (11.1) implies r_0 divides h_0^2; so $h_0 = 1$ implies $r_0 = h_0$, contradicting Lemma 11.1. We can now assume $r_0 > h_0 > 1$ as starting point and inductively define r_n and h_n.
If $n \geq 0, |r_n| > |h_n| > 1$ and r_n is a root of

$$P_n(R) = R^2 - 2Ry(h_n - \epsilon) - h_n^2, \tag{11.2}$$

we define r_{n+1} to be the other root of $P_n(R)$:

$$r_{n+1} = -r_n + 2y(h_n - \epsilon). \tag{11.3}$$

Then

$$|r_n||r_{n+1}| = h_n^2,$$

so $1 \leq |r_{n+1}| < |h_n|$.

If $|r_{n+1}| = 1$. then $r_n \equiv \pm 1 \pmod{2y}$ and by (11.3) it follows inductively that $r_0 \equiv \pm 1 \pmod{2y}$. Hence $\gcd(r_0, y) = 1$ and hence $\gcd(x, y) = 1$ and we exit the algorithm. We note for future reference that r_0 is odd in this case.

Otherwise we assume $|r_{n+1}| > 1$ and define the polynomial

$$Q_n(H) = H^2 + 2r_{n+1}yH - 2r_{n+1}y\epsilon - r_{n+1}^2. \tag{11.4}$$

Then $Q_n(h_n) = 0$ and we let h_{n+1} be the other root of $Q_n(H)$:

$$h_{n+1} = -h_n - 2r_{n+1}y. \tag{11.5}$$

Then

$$h_{n+1}^2 + 2r_{n+1}yh_{n+1} - 2r_{n+1}y\epsilon - r_{n+1}^2 = 0. \tag{11.6}$$

We note that $|h_{n+1}| = 1$ implies $|r_{n+1}| = 1$, as by (11.6), r_{n+1} divides h_{n+1} and as previously, we exit the algorithm with $\gcd(x, y) = 1$.

Let $H_n = h_n - \epsilon$ and $H_{n+1} = h_{n+1} - \epsilon$. Then

$$\begin{aligned} H_nH_{n+1} &= h_nh_{n+1} - \epsilon(h_n + h_{n+1}) + 1 \\ &= -2r_{n+1}y\epsilon - r_{n+1}^2 + 2r_{n+1}y\epsilon + 1 \\ &= 1 - r_{n+1}^2. \end{aligned}$$

Then $|H_n||H_{n+1}| = r_{n+1}^2 - 1 > 0$. Also

$$|H_n| = |h_n - \epsilon| \geq |h_n| - 1 \geq |r_{n+1}|.$$

Hence

$$|h_{n+1} - \epsilon| = |H_{n+1}| = \frac{r_{n+1}^2 - 1}{|H_n|} \leq \frac{r_{n+1}^2 - 1}{|r_{n+1}|} < |r_{n+1}|,$$

so $|h_{n+1}| \leq |r_{n+1}|$. Assume $|h_{n+1}| = |r_{n+1}|$. Then (11.6) implies

$$2r_{n+1}yh_{n+1} = 2r_{n+1}y\epsilon$$

and hence $h_{n+1} = \epsilon$. But this gives the contradiction

$$|r_{n+1}| = |h_{n+1}| = 1.$$

If $h_{n+1} = 0$, then (11.6) implies $-2r_{n+1}y\epsilon - r_{n+1}^2 = 0$, so $r_{n+1} = -2y\epsilon$. Then as $r_n + r_{n+1} = 2y(h_n - \epsilon)$, it follows that $r_0 \equiv 0 \pmod{2y}$. Then

y divides r_0 and hence x and we exit the algorithm. We note for future reference that in this case, r_0 is even.

Hence we can assume $|r_{n+1}| > |h_{n+1}| > 1$ and the induction proceeds. As $|r_n|$ and $|h_n|$ strictly decrease, we must eventually reach one of $|r_n| = 1$ or $h_n = 0$. ∎

Corollary 11.3. *For a Type 1 solution (x, y) of (1.1), if $y > 1$ and $\gcd(x, y) = 1$, then $r = u^2$, where u is odd and $k = uv$, where $\gcd(u, v) = 1$ and $v > u > 1$. Also*

$$v^2 - (y^2 + 1)u^2 = 2y\epsilon. \tag{11.7}$$

Proof. We saw in the proof of Theorem 11.2, that either $r \equiv \pm 1 \pmod{2y}$ or $r \equiv 0 \pmod{2y}$. Hence if $\gcd(x, y) = 1$ and $y > 1$, then $r \equiv x \not\equiv 0 \pmod{y}$, so we must have $r \equiv \pm 1 \pmod{2y}$ and hence r is odd. Then parts (i) and (ii) of Lemma 10.2 give $r = u^2$, where $k = uv$ and $\gcd(u, v) = 1$. Also

$$s^2 - 1 = k^2 - r^2 = u^2v^2 - u^4. \tag{11.8}$$

Then, as $s > 1$, (11.8) gives $u^2v^2 - u^4 > 0$ and hence $v > u$.

Finally, $s = yr + \epsilon = yu^2 + \epsilon$, so

$$s^2 - 1 = u^2(y^2u^2 + 2y\epsilon). \tag{11.9}$$

Then (11.8) and(11.9) give

$$v^2 - (y^2 + 1)u^2 = 2y\epsilon.$$

∎

We can now derive explicit formulae for x, y and k for a Type 1 solution (x, y) with $\gcd(x, y) = 1$ and $y > 1$.

THEOREM 11.4. *If* (x, y) *is a Type* 1 *exceptional solution of equation* (1.1)*, with* $\gcd(x, y) = 1$ *and* $y > 1$*, then* $k = u_n v_n$*, where*

$$v_n + u_n\sqrt{y^2+1} = f(g(y+\epsilon) + \sqrt{y^2+1})(2y^2+1+2y\sqrt{y^2+1})^n, \tag{11.10}$$

where $n \geq 1$ *and one of the following four possibilities holds:*

(a) $f = g = 1, \epsilon = 1$*;*
(b) $f = g = 1, \epsilon = -1$*;*
(c) $f = 1, g = -1, \epsilon = -1$*;*
(d) $f = g = -1, \epsilon = 1$.

PROOF. Assume (x, y) is a Type 1 exceptional solution of equation (1.1), with $\gcd(x, y) = 1$ and $y > 1$. Then by Corollary 11.3 and equation 11.7, $k = uv$, where

$$v^2 - (y^2+1)u^2 = 2y\epsilon.$$

Then Lemma 3.6 of [8] implies

$$v + u\sqrt{y^2+1} = f(g(y+\epsilon) + \sqrt{y^2+1})(2y^2+1+2y\sqrt{y^2+1})^n, \tag{11.11}$$

where $f = \pm 1, g = \pm 1, n$ an integer. Clearly $n \neq 0$ as $n = 0$ implies $u = 1$.

This gives 16 possibilities for f, g, ϵ and the sign of n as in Table 2. We then eliminate all 8 cases where $n < 0$. Of the 8 cases where $n \geq 1$, only (a)–(d) remain. See section 12 for the proof of one case with $n > 0$ and for one case with $n < 0$. ∎

n	f	g	ϵ	v	u
$+$	1	1	1	$+$	$+$
$+$	1	1	-1	$+$	$+$
$+$	1	-1	-1	$+$	$+$
$+$	-1	-1	1	$+$	$+$
$+$	1	-1	1	$-$	$-$
$+$	-1	1	1	$-$	$-$
$+$	-1	1	-1	$-$	$-$
$+$	-1	-1	-1	$-$	$-$
$-$	1	1	1	$+$	$-$
$-$	1	1	-1	$-$	$+$
$-$	1	-1	1	$-$	$+$
$-$	1	-1	-1	$-$	$+$
$-$	-1	1	1	$-$	$+$
$-$	-1	1	-1	$+$	$-$
$-$	-1	-1	1	$+$	$-$
$-$	-1	-1	-1	$+$	$-$

TABLE 2. The 16 sign possibilities in (11.11).

12. Two examples of sign determination

(1) We prove that if $n \geq 1$ and $f = 1, g = -1, e = 1$, then v and u given by (11.10) satisfy $v < 0$ and $u < 0$. Let

$$v_n + u_n\sqrt{y^2+1} = (-(y+1) + \sqrt{y^2+1})(2y^2+1+2y\sqrt{y^2+1})^n.$$

Then $v_1 = -(2y^2 - y + 1) < 0, u_1 = -(2y-1) < 0$. Also

$$v_{n+1} = (2y^2+1)v_n + 2yu_n, \quad u_{n+1} = 2yv_n + (2y^2+1)u_n.$$

It follows by induction on $n \geq 1$ that $v_n < 0$ and $u_n < 0$.

(2) We prove that if $n = -N < 0$ and $f = 1, g = 1, e = 1$, then v and u given by (11.10) satisfy $v > 0$ and $u < 0$. Let $v'_N = v_n, u'_N = u_n$.

$$v'_N + u'_N\sqrt{y^2+1} = (y + 1 + \sqrt{y^2+1})(2y^2 + 1 - 2y\sqrt{y^2+1})^N.$$

Then $v'_1 = 2y^2 - y + 1 > 0, u'_1 = -(2y - 1) < 0$. Also

$$v'_{N+1} = (2y^2 + 1)v'_N - 2yu'_N, \quad u'_{N+1} = -2yv'_N + (2y^2 + 1)u'_N.$$

It follows by induction on $N \geq 1$ that $v'_N > 0$ and $u'_N < 0$.

13. Removal of parameters f and g

Let $D = y^2 + 1$. Then equation (11.10) with conjugation gives

$$v_n + u_n\sqrt{D} = (a + b\sqrt{D})\alpha^n \tag{13.1}$$

$$v_n - u_n\sqrt{D} = (a - b\sqrt{D})\beta^n, \tag{13.2}$$

where $a = fg(y + \epsilon), b = f$ and

$$\alpha = 2y^2 + 1 + 2y\sqrt{D}, \quad \beta = 2y^2 + 1 - 2y\sqrt{D}. \tag{13.3}$$

Note that $\alpha\beta = 1$. First we remove f.

Lemma 13.1. *If (k, x, y) is a Type 1 exceptional solution satisfying* $\gcd(x, y) = 1, y > 1$*, then $(x, k) = (x_n, k_n)$, where*

$$x_n + k_n\sqrt{D} = (y^2 + \epsilon y + 1 + g(y + \epsilon)\sqrt{D})\alpha^{2n}, n \geq 1, \tag{13.4}$$

and $g = \pm 1, \epsilon = \pm 1$.

PROOF. We know that

$$\begin{aligned}
x_n + k_n &= u_n^2 D + y\epsilon + v_n u_n \sqrt{D} \\
&= u_n\sqrt{D}(v_n + u_n\sqrt{D}) + y\epsilon \\
&= \frac{((a+b\sqrt{D})\alpha^n - (a-b\sqrt{D})\beta^n)}{2}(a+b\sqrt{D})\alpha^n + y\epsilon \\
&= \frac{(a+b\sqrt{D})^2}{2}\alpha^{2n} - \frac{(a^2-b^2D)}{2} + y\epsilon \\
&= \frac{(a+b\sqrt{D})^2}{2}\alpha^{2n} \\
&= \frac{(fg(y+\epsilon)+f\sqrt{D})^2}{2}\alpha^{2n} \\
&= \frac{((y+\epsilon)^2 + 2g(y+\epsilon)\sqrt{D} + y^2+1}{2}\alpha^{2n} \\
&= (y^2+\epsilon y + 1 + g(y+\epsilon)\sqrt{D})\alpha^{2n}.
\end{aligned}$$

□

Now we remove g.

COROLLARY 13.2. *If (k, x, y) is a Type 1 exceptional solution with* $\gcd(x, y) = 1, y > 1$*, then $(x, k) = (X_m, K_m)$, where*

$$X_m + K_m\sqrt{D} = (y^2 + \epsilon y + 1 + (y+\epsilon)\sqrt{D})\alpha^m, \tag{13.5}$$

where $m \geq 1$ and $\epsilon \pm 1$. Conversely if (X_m, K_m) is given by (13.5), where $y > 1$, then (K_m, X_m, y) is a Type 1 exceptional solution with $\gcd(X_m, y) = 1$.

PROOF. If $g = 1$, formula 13.4 gives

$$x_n + k_n\sqrt{D} = (y^2 + \epsilon y + 1 + (y+\epsilon)\sqrt{D})\alpha^{2n}. \tag{13.6}$$

If $g = -1$, formula 13.4 gives

$$\begin{aligned}
x_n + k_n &= (y^2 + \epsilon y + 1 - (y+\epsilon)\sqrt{D})\alpha^{2n} \\
&= (y^2 + \epsilon y + 1 - (y+\epsilon)\sqrt{D})\alpha^{2n-1}\alpha \\
&= (y^2 + \epsilon y + 1 - (y+\epsilon)\sqrt{D})(2y^2 + 1 + 2y\sqrt{D})\alpha^{2n-1} \\
&= (y^2 - \epsilon y + 1 + (y-\epsilon)\sqrt{D})\alpha^{2n-1}. \qquad (13.7)
\end{aligned}$$

Then (13.6) and (13.7) combine into one formula (13.5).

Conversely, formula (13.5) implies

$$X_m \equiv (-1)^m \epsilon y \pmod{y^2+1}.$$

Also $X_m > 0, K_m > y + 1, \gcd(X_m, K_m) = 1$ all follow by induction, using the recurrence relations

$$\begin{aligned}
X_{m+1} &= (2y^2+1)X_m + 2yDK_m \\
K_{m+1} &= (2y^2+1)K_m + 2yX_m.
\end{aligned}$$

□

14. Constructing exceptional solutions

The construction starts from the following *trivial* solutions:

(i) $(t, t, 0), t \geq 2$,

(ii) $(t, t^2 - t + 1, t - 1), t \geq 2$,

(iii) $(t, t^2 + t + 1, t + 1), t \geq 1$.

Definition 14.1. *Let* (k, x, y) *be a solution of* (1.1). *Then*

(i) $g_+(k, x, y) = (K, X, Y)$, *where*

$$X + K\sqrt{k^2+1} = (x + y\sqrt{k^2+1})(2k^2 + 1 + 2k\sqrt{k^2+1}). \qquad (14.1)$$

(ii) $g_0(k,x,y) = (K,X,Y)$, *where*

$$X + K\sqrt{y^2+1} = (x + k\sqrt{y^2+1})(2y^2 + 1 + 2y\sqrt{y^2+1}). \tag{14.2}$$

(iii) $g_-(k,x,y) = (K,X,Y)$, *where*

$$X + K\sqrt{k^2+1} = (x - y\sqrt{k^2+1})(2k^2 + 1 + 2k\sqrt{k^2+1}). \tag{14.3}$$

REMARK 14.2. In all three cases $\gcd(X,Y) = gcd(x,y)$.

LEMMA 14.3. *Suppose (k,x,y) is an exceptional solution of (1.1). Then $g_+(k,x,y), g_0(k,x,y)$ and $g_-(k,x,y)$ are exceptional solutions. Morever with $T = (2Y^2+1)K - 2YX$,*

(i) $g_+(k,x,y) = (K,X,Y)$ *where* $0 < T < Y - 1$.
(ii) $g_0(k,x,y) = (K,X,Y)$ *where* $Y + 1 < T$.
(iii) $g_-(k,x,y) = (K,X,Y)$ *where* $-(Y-1) < T < 0$.

In all cases, we have $K > k$.

PROOF. (i) We have

$$K = 2kx + (2k^2+1)y, \quad X = (2k^2+1)x + (k^2+1)2ky, \quad Y = k.$$

Taking norms in (14.1) gives $X^2 - (k^2+1)K^2 = x^2 - (k^2+1)y^2 = k^2$, so $X^2 - (Y^2+1)K^2 = Y^2$.

Also $K > 2k \geq k+1 = Y+1$, $X > 0$ and hence (K,X,Y) is an exceptional solution. Next, $0 < y < k-1, y = (2Y^2+1)K - 2YX = T$, so $0 < T < Y - 1$. Clearly $K > k$ here.

(ii) We have

$$K = 2yx + (2y^2+1)k, \quad X = (2y^2+1)x + (y^2+1)2yk, \quad Y = y.$$

Taking norms in (14.2) gives $X^2 - (y^2+1)K^2 = x^2 - (y^2+1)k^2 = y^2$, so $X^2 - (Y^2+1)K^2 = Y^2$.

Also $K > 2y^2 + 1 > y + 1 = Y + 1$, $X > 0$ and hence (K, X, Y) is an exceptional solution. Next, $y + 1 < k, k = (2Y^2 + 1)K - 2YX = T$, so $Y + 1 < T$. Clearly $K > k$ here.

(iii) We have

$$K = 2kx - (2k^2 + 1)y, \quad X = (2k^2 + 1)x - (k^2 + 1)2ky, \quad Y = k.$$

Taking norms in (14.3) gives $X^2 - (k^2 + 1)K^2 = x^2 - (k^2 + 1)y^2 = k^2$, so $X^2 - (Y^2 + 1)K^2 = Y^2$. Also

$$\begin{aligned} X &> (2k^2 + 1)y\sqrt{k^2 + 1} - (k^2 + 1)2ky \\ &= y(2k^2 + 1 - 2k\sqrt{k^2 + 1})\sqrt{k^2 + 1} > 0. \end{aligned}$$

We now have to prove $K > Y + 1 = k + 1$, i.e.,

$$2kx > (2k^2 + 1)y + k + 1.$$

On squaring both sides, using $x^2 = (k^2 + 1)y^2 + k^2$, this becomes

$$4k^4y^2 + 4k^2y^2 + 4k^4 > (2k^2 + 1)^2y^2 + 2(2k^2 + 1)y(k + 1) + (k + 1)^2. \tag{14.4}$$

Inequality (14.4) reduces to

$$4k^4 > y^2 + 2(2k^2 + 1)y(k - 1) + (k + 1)^2. \tag{14.5}$$

However the RHS of (14.5) is $< 4(k^4 - 2k^3 + 2k^2 - k + 1) < 4k^4$, if $k > 1$. Hence (K, X, Y) is an exceptional solution.
Finally, as $-(k - 1) < -y < 0$ and $y = -(2Y^2 + 1)K + 2YX = -T$, we have $-(Y - 1) < T < 0$. Also $K > k$ here. ☐

Lemma 14.4. *Let* $T = (2Y^2 + 1)K - 2YX$.

(i) *If* $t \geq 2$, *then* $g_+(t, t, 0) = (K, X, Y)$, *where* $T = 0$.
(ii) *If* $t \geq 2$, *then* $g_+(t, t^2 - t + 1, t - 1) = (K, X, Y)$, *where* $T = Y - 1$.

(iii) *If* $t \geq 1$, *then* $g_+(t, t^2+t+1, t+1) = (K, X, Y)$, *where* $T = Y+1$.

In each case (K, X, Y) *is an exceptional solution.*

PROOF. (i) $g_+(t, t, 0) = (2t^2, 2t^3 + t, t) = (K, X, Y)$.

Then $K = 2t^2, X = 2t^3 + t, Y = t$ and

$$\begin{aligned} T &= (2Y^2 + 1)K - 2YX \\ &= (2t^2 + 1)2t^2 - 2t(2t^3 + t) = 0. \end{aligned}$$

Also if $t \geq 2$, then $Y = t < 2t^2 - 1 = K - 1$, so (K, X, Y) is an exceptional solution. Similarly for (ii) and (iii). ∎

COROLLARY 14.5. *If* x_n *and* k_n *are defined for* $n \geq 1$ *by*

$$x_n + k_n\sqrt{t^2 + 1} = t(2t^2 + 1 + 2t\sqrt{t^2 + 1})^n, \tag{14.6}$$

where $t \geq 2$, *then*

(i) $(k_1, x_1, t) = g_+(t, t, 0)$

(ii) $(k_{n+1}, x_{n+1}, t) = g_0(k_n, x_n, t)$

(iii) (k_n, x_n, t) *is an exceptional solution for* $n \geq 1$.

PROOF. (i) $g_+(t, t, 0) = (2t^2, 2t^3 + t, t) = (k_1, x_1, t)$.

(ii) From (14.6), we have recurrence relations

$$\begin{aligned} x_{n+1} &= (2t^2 + 1)x_n + (t^2 + 1)2tk_n \\ k_{n+1} &= 2tx_n + (2t^2 + 1)k_n. \end{aligned}$$

Hence

$$\begin{aligned} g_0(k_n, x_n, t) &= (2tx_n + (2t^2 + 1)k_n, (2t^2 + 1)x_n + (t^2 + 1)2tk_n, t) \\ &= (k_{n+1}, x_{n+1}, t) \end{aligned}$$

(iii) We use induction on $n \geq 1$. We know (k_1, x_1, t) is an exceptional solution. Now assume (k_n, x_n, t) is an exceptional solution. Then Lemma 14.3 shows that (k_{n+1}, x_{n+1}, t) is also an exceptional solution. ∎

In a similar fashion, we have

COROLLARY 14.6. *If x_n and k_n are defined for $n \geq 1$ by*

$$x_n + k_n\sqrt{t^2+1} = (t^2 + \epsilon t + 1 + (t+\epsilon)\sqrt{t^2+1})(2t^2 + 1 + 2t\sqrt{t^2+1})^n,$$

where $t \geq 1$ if $\epsilon = 1$ and $t \geq 2$ if $\epsilon = -1$, then

(i) $(k_1, x_1, t) = g_+(t, t^2 + \epsilon t + 1, t + \epsilon)$

(ii) $(k_{n+1}, x_{n+1}, t) = g_0(k_n, x_n, t)$

(iii) (k_n, x_n, t) *is an exceptional solution for* $n \geq 1$.

REMARK 14.7. Recall that an exceptional solution (k, x, y) is of Type 1, if $y^2 + 1$ divides $x + y$ or $x - y$. Any other exceptional solution is called Type 2. Then we proved earlier that the exceptional solutions (k_n, x_n, t) in Corollary 14.5 are the (k, x, y) for which y divides x and $y > 1$ and that these are Type 1 solutions. Contrastingly, those in Corollary 14.6 are the Type 1 exceptional solutions (k, x, y) for which $\gcd(x, y) = 1$.

LEMMA 14.8. (i) *Suppose that (k, x, y) is an exceptional solution. Then $g_+(k, x, y)$ and $g_-(k, x, y)$ are Type 2 exceptional solutions.*

(ii) *Suppose that (k, x, y) is a Type 2 exceptional solution. Then $g_0(k, x, y)$ is a Type 2 exceptional solution.*

PROOF. (i) $g_+(k, x, y)$ and $g_-(k, x, y)$ have the form (Y, X, k), with $X = Rx + eDSy, e = \pm 1$. We have to prove that $X \pm k$ are not divisible by k^2+1.

$$X - k = Rx + eDSy - k \equiv -x - k \pmod{k^2+1},$$

$$X + k = Rx + eDSy + k \equiv -x + k \pmod{k^2+1}.$$

Also $x < k^2 - k + 1$, as $y < k - 1$. Also $x \neq k$ here. So

$$0 < |x - k| < x + k < k^2 + 1$$

and neither $x - k$ nor $x + k$ is divisible by $k^2 + 1$.

(ii) Suppose (k, x, y) is a Type 2 exceptional solution. Then

$$\begin{aligned} g_0(k,x,y) &= (2yx + (2y^2+1)k, (2y^2+1)x + (y^2+1)2yk, y) \\ &= (K, X, Y). \end{aligned}$$

$$\begin{aligned} \text{Then } Y = y \text{ and } X \pm Y &= (2y^2+1)x + (y^2+1)2y \pm y \\ &\equiv -x \pm y \not\equiv 0 \pmod{y^2+1}. \end{aligned}$$

□

15. The recursive construction

In the previous section, we have established the following. Let $\mathscr{E}$ be the set of exceptional solutions (k, x, y). Then with $R = 2Y^2 + 1, S = 2Y$ and $T = RK - SX$,

(i) g_0 maps $\mathscr{E}$ 1–1 into $\{(K, X, Y) \in \mathscr{E} | Y + 1 < T\}$.

(ii) g_+ maps $\mathscr{E}$ 1–1 into $\{(K, X, Y) \in \mathscr{E} | 0 < T < Y - 1\}$.

(iii) g_- maps $\mathscr{E}$ 1–1 into $\{(K, X, Y) \in \mathscr{E} | -(Y-1) < T < 0\}$.

(iv) g_+ maps $\{(t, t, 0) | t \geq 2\}$ 1–1 into $\{(K, X, Y) \in \mathscr{E} | T = 0\}$.

(v) g_+ maps $\{(t, t^2 - t + 1, t - 1) | t \geq 2\}$ 1–1 into $\{(K, X, Y) \in \mathscr{E} | T = Y - 1\}$.

(vi) g_+ maps $\{(t, t^2+t+1, t+1) | t \geq 1\}$ 1–1 into $\{(K, X, Y) \in \mathscr{E} | T = Y + 1\}$.

It is easy to check that these mappings are surjective.

We construct a forest of exceptional solutions, as follows. We start from an exceptional solution obtained by applying g_+ to each of the trivial solutions (i) $(t, t, 0), t \geq 2$, (ii) $(t, t^2 - t + 1, t - 1), t \geq 2$, (iii) $(t, t^2+t+1, t+1), t \geq 1$. Then recursively, from an exceptional solution (k, x, y), we produce three further exceptional solutions.

Because of Remark 14.2, the solutions in trees with root node (i) will have $\gcd(x, y) = t \geq 2$, while those with root node (ii) or (iii), will have $\gcd(x, y) = 1$.

Figures 1–3 give fragments of the forest of exceptional solutions.

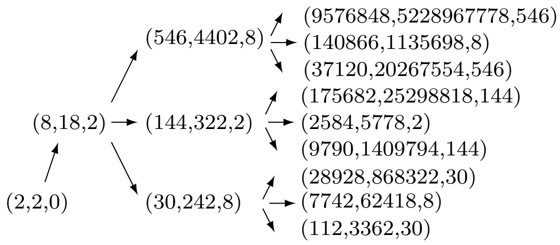

FIGURE 1. Tree fragment starting from $(t, t, 0) = (2, 2, 0)$.

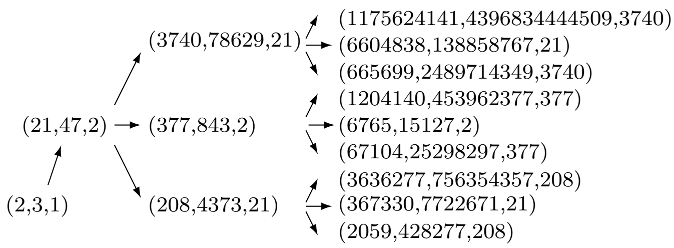

FIGURE 2. Tree fragment starting from $(t, t^2 - t + 1, t - 1) = (2, 3, 1)$.

We now show that all exceptional solutions occur in the forest and are

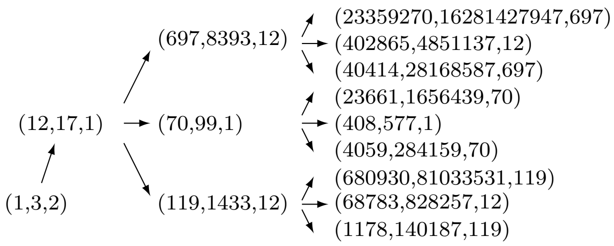

FIGURE 3. Tree fragment starting from $(t, t^2 + t + 1, t + 1) = (1, 3, 2)$.

reached by a unique path from a root node.

LEMMA 15.1. *If (K, X, Y) is an exceptional solution and $T = RK - SX$ where $R = 2Y^2 + 1$ and $S = 2Y$, then*

(a) $-(Y-1) < T$,
(b) $T \neq Y$.

PROOF. First we prove (a).

$$\begin{aligned} -(Y-1) < T &\iff -T = SX - RK < Y - 1 \\ &\iff 2YX < (2Y^2+1)K + Y - 1 \\ &\iff 4Y^2X^2 < (4Y^4 + 4Y^2 + 1)K^2 + 2K(2Y^2+1)(Y-1) + (Y-1)^2 \\ &\iff 4Y^4 < K^2 + 2K(2Y^2+1)(Y-1) + (Y-1)^2. \end{aligned}$$

However, the last inequality follows from $K > Y + 1$, as

$$\begin{aligned} &K^2 + 2K(2Y^2+1)(Y-1) + (Y-1)^2 \\ &\qquad > (Y+1)^2 + 2(2Y^2+1)(Y^2-1) + (Y-1)^2 \\ &\qquad = 4Y^4. \end{aligned}$$

(b) Now assume $T = Y$. Then $(2Y^2 + 1)K - 2YX = Y$, so Y divides K. Hence Y divides X. Let $K = YW$ and $X = YZ$. Then

$$(2Y^2 + 1)W - 2YZ = 1$$
$$Z^2 - (Y^2 + 1)W^2 = 1.$$

Eliminating Z gives $4Y^2(W + 1) = (W - 1)^2$. Hence W is odd, $W = 2U+1$ and $2Y^2(U+1) = U^2$. Then $U+1$ divides U^2, which contradicts $\gcd(U + 1, U^2) = 1$. ∎

Definition 15.2. *Let (K, X, Y) be an exceptional solution. Let $R = 2Y^2 + 1, S = 2Y, D = Y^2 + 1$ and $T = RK - SX$. Then*

$$h(K, X, Y) = \begin{cases} g_0^{-1}(K, X, Y) & \text{if } Y + 1 < T \\ g_+^{-1}(K, X, Y) & \text{if } 0 \le T \le Y + 1, T \ne Y \\ g_-^{-1}(K, X, Y) & \text{if } -(Y - 1) < T < 0. \end{cases} \tag{15.1}$$

Remark 15.3. By virtue of Lemma 15.1, h is well–defined and $h(K, X, Y) = (k, x, y)$ is either an exceptional solution with $k < K$, or one of the trivial solutions $(Y, Y^2 + \epsilon Y + 1, Y + \epsilon)$ or $(Y, Y, 0)$.

It follows that repeated application of h on an exceptional solution $K, X, Y)$ will eventually reach a trivial solution (k, x, y) and consequently (K, X, Y) occurs in the tree whose root node is (k, x, y). As the path from (K, X, Y) back to a root node is uniquely defined, the forest of exceptional solutions contains every exceptional solution just once. Dujella's conjecture means that no two nodes can have the same K.

The forest can be used to check that Dujella's conjecture holds for all k not exceeding a given bound. For as one travels along a path from a root node, the value of k increases; also as t is increased in one the three types of root node (k, x, y), so does the size of K, where $g_+(k, x, y) = (K, X, Y)$.

It is clear by induction that the exceptional solutions have the form $(K(t), X(t), Y(t))$, where the components are polynomials with integer coefficients, corresponding to the three types of root nodes: $(t, t, 0), t \geq 2, (t, t^2 - t + 1, t - 1), t \geq 2$ and $(t, t^2 - t + 1, t - 1), t \geq 1$.

16. Families of k with explicit exceptional solutions

The following examples were suggested by an extension of Table 1 to $k \leq 2^{32}$. We use the terminology of Proposition 2.1. The continued fraction identities were proved using formula (iv) of Lemma 6.3.

Example 16.1. $g_+(t, t, 0) = (k, x, y) = (2t^2, 2t^3 + t, t), t \geq 2$. Then

$$d = t, a = 2t^2 + 2t + 1, b = 2t^2 - 2t + 1, p = 1, q = 1.$$

Then

$$\sqrt{b/a} = [0, 1, \overline{t - 1, 1, 1, t - 1, 2}], \text{ period length 5.}$$

Also $Q_2 = 4t = 2k/d$ and $p/q = A_1/B_1$.

t	2	3	4	5
k	8	18	32	50

Example 16.2. $g_0 g_+(t, t, 0) = (k, x, y) = (8t^4 + 4t^2, 8t^5 + 8t^3 + t, t)$, where $t \geq 2$. Then

$$d = t, a = 8t^4 + 8t^3 + 8t^2 + 4t + 1, b = 8t^4 - 8t^3 + 8t^2 - 4t + 1, p = 1, q = 1.$$

Then

$$\sqrt{b/a} = [0, 1, \overline{t - 1, 1, 1, t - 1, 1, 1, t - 1, 1, 1, t - 1, 2}], \text{ period length 11.}$$

Also $Q_2 = 16t^3 + 8t = 2k/d$ and $p/q = A_1/B_1$.

t	2	3	4	5
k	144	684	2112	5100

EXAMPLE 16.3. $g_+(t, t^2 + t + 1, t + 1) = (k, x, y), t \geq 1$. Then

$$k = 4t^3 + 4t^2 + 3t + 1, \quad x = 4t^4 + 4t^3 + 5t^2 + 3t + 1, y = t$$

and $d = 1$ if t is odd, whereas $d = 2$ if t is even.

$$a = \begin{cases} (4t^4 + 8t^3 + 9t^2 + 6t + 2)/2 & \text{if } t \text{ is even} \\ 4t^4 + 8t^3 + 9t^2 + 6t + 2 & \text{if } t \text{ is odd.} \end{cases}$$

$$b = \begin{cases} 8t^2 + 2 & \text{if } t \text{ is even} \\ 4t^2 + 1 & \text{if } t \text{ is odd.} \end{cases}$$

Then $p = 1$ and $q = t/2$ if t is even, whereas $q = t$ if t is odd.

(i) If t is even,

$$\sqrt{b/a} = [0, t/2, \overline{1, 1, t-1, 1, 1, t-1, 1, 1, t}], \text{ period length 9.}$$

Also $Q_2 = 4t^3 + 4t^2 + 3t + 1 = k = 2k/d$ and $p/q = A_1/B_1$.

(ii) If t is odd,

$$\sqrt{b/a} = [0, t+1, \overline{2t, 2t, 2t+2}], \text{ period length 3.}$$

Also $Q_1 = b = 4t^2 + 1, Q_2 = 4t^2 + 4t + 1, P_2 = 4t^3 + 4t^2 + t + 1$.

Hence $Q_2 - Q_1 + 2P_2 = 2k$ and $p/q = (A_1 - A_0)/(B_1 - B_0)$.

t	1	2	3	4	5
k	12	55	154	333	616

Acknowledgments

The first author thanks Alan Offer for valuable discussions concerning the construction of the forest. Also the manuscript has been greatly improved by suggestions from Professor Andrej Dujella.

References

[1] L. E. Dickson, *Introduction to the theory of numbers*, Dover Publications, 1957.

[2] A. Dujella, Continued fractions and RSA with small secret exponent, *Tatra Mt. Math. Publ.* 29 (2004), 101–112.

[3] A. Dujella, Clemens Fuchs, Complete solution of a problem of Diophantus and Euler, *J. London Math. Soc,*, 71 (2005), 33–52.

[4] A. Dujella, B. Jadrijević, A family of quartic Thue inequalities, *Acta Arith.* 111 (2004), 61–76.

[5] A. Filipin, Y. Fujita, M. Mignotte, The non-extendibility of some parametric families of $D(1)$–triples, *Quarterly J. Math.* 63 (2012), 605–621.

[6] Y. Fujita, The non-extensibility of $D(4k)$–triples $\{1, 4k(k-1), 4k^2+1\}$ with $|k|$ prime, *Glasnik. Math.*, 2006, 205–216.

[7] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner, 1954.

[8] P.Z. Yuan, Z.F. Zhang, On the diophantine equation $X^2 - (1+a^2)Y^4 = -2a$, *Sci. China Math.*, 2010, 53(8), 2143–2158.

K.R. Matthews
Department of Mathematics
University of Queensland
Brisbane, Australia, 4072
and
Centre for Mathematics and its Applications
Australian National University
Canberra, ACT, Australia, 0200
E-mail: keithmatt@gmail.com

J.P. Robertson

Actuarial and Economic Services Division

National Council on Compensation Insurance

Boca Raton, FL 33487

E-mail: jpr2718@gmail.com

J. White

14 Nash Place, Stirling,

Canberra, ACT, Australia, 2611

E-mail: mathimagics@yahoo.co.uk