On a diophantine equation of Andrej Dujella

Keith Matthews

(joint work with John Robertson and Jim White published in
Math. Glasnik, 48, number 2 (2013) 265-289.)

The unicity conjecture (Dujella 2009)

Let $k \geq 2, k \in \mathbb{N}$. Then the diophantine equation

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

has at most one positive solution (x, y) with $y < k - 1$. We call such a solution an *exceptional* solution.

Example. $k = 8$ is the first k possessing an exceptional solution, namely $(x, y) = (18, 2)$.

We have verified the conjecture for $k \leq 2^{50}$.

Cases for which the conjecture has been proved

The conjecture has been proved in the following cases:
Filipin, Fujita and Mignotte:

(a) $k^2 + 1 = p^n$ or $2p^n$, p an odd prime: no exceptional solutions.

(b) $k = p^{2i}$ or p^{2i+1} or $2p^{2i+1}$, p an odd prime: no exceptional solutions.

(c) $k = 2p^{2i}, p$ an odd prime: the exceptional solution is $(2p^{3i} + p^i, p^i)$.

Matthews and Robertson: $k^2 + 1 = p^m q^n$ or $2p^m q^n, m, n \geq 1$, p and q distinct odd primes.

The $D(-1)$ 4–tuples conjecture

This states that there do not exist four positive integers such that the product of any two is one plus a square.

The unicity conjecture implies the $D(-1)$ 4–tuples conjecture (Dujella)

Assume the unicity conjecture and let a, b, c, d be a $D(-1)$-quadruple with $0 < a < b < c < d$. Then $a = 1$ by Dujella-Fuchs (J. London Math. Soc. 2005) and hence

$$b = r^2 + 1, c = s^2 + 1, d = t^2 + 1.$$

Now consider the equation $(y^2 + 1)(t^2 + 1) = x^2 + 1$, i.e.,

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

By the conjecture, this diophantine equation has at most one solution with $0 < y < t - 1$.

But by assumption, it has at least two solutions with $0 < y < t$, namely, $y = r$ and $y = s$, and hence we must have $s = t - 1$.

However this contradicts a *gap* property (Dujella-Fuchs, Lemma 9) which implies that $d > c^2$, because the inequality

$$d = t^2 + 1 > c^2 = ((t - 1)^2 + 1)^2$$

does not hold for any $t > 2$.

Type 1 and Type 2 solutions

Dujella's equation can be written as

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

We divide the exceptional solutions into two classes:

The Type 1 solutions are those for which $y^2 + 1$ divides $x + y$ or $x - y$, while Type 2 solutions are the remaining ones.

In the range $k \leq 2^{50}$, there are $23,862,782$ Type 1 and $73,034$ Type 2 exceptional solutions.

Characterisation of Type 1 solutions

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

$$r^2 + s^2 = k^2 + 1$$
$$s \equiv \epsilon \pmod{r},$$

namely

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

where we take $\epsilon = 1$ if $y = 1$.

Example. $k = 8, (x, y) = (18, 2), \epsilon = -1, (r, s) = (4, 7)$.

Example 1: Type 1(a) exceptional solution

These are the (k_n, x_n, y), where

$$x_n + k_n\sqrt{D} = y(R + S\sqrt{D})^n, n \geq 1,$$

and $R = 2y^2 + 1, S = 2y, D = y^2 + 1$ and $y \geq 2$.

Here

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

and y divides x_n.

Example 2: Type 1(b) exceptional solution

These are the (k_n, x_n, y), where

$$x_n + k_n\sqrt{D} = (y^2 + \epsilon y + 1 + (y + \epsilon)\sqrt{D})(R + S\sqrt{D})^n, n \geq 1,$$

and where $y \geq 1$ if $\epsilon = 1$ and $y \geq 2$ if $\epsilon = -1$.

Here

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

and $\gcd(x_n, y) = 1$.

Types 1(a) and 1(b) give all Type 1 solutions

Theorem. If (k, x, y) is a Type 1 solution, then

(i) either (a) y divides x and $y > 1$, or (b) $\gcd(x, y) = 1$.

(ii) (k, x, y) is a Type 1(a) solution in case (a) and a Type 1(b) solution in case (b).

Producing exceptional solutions

The following three functions each create an exceptional solution (K_i, X_i, Y_i) from an exceptional solution (k, x, y):

(i) $g_+(k, x, y) = (K_1, X_1, Y_1)$, $Y_1 = k$,

(ii) $g_-(k, x, y) = g_+(k, x, -y) = (K_2, X_2, Y_2)$, $Y_2 = k$,

(iii) $g_0(k, x, y) = g_+(y, x, k) = (K_3, X_3, Y_3)$, $Y_3 = y$,

where

$$X_1 + K_1\sqrt{k^2+1} = (x + y\sqrt{k^2+1})(2k^2 + 1 + 2k\sqrt{k^2+1})$$
$$X_2 + K_2\sqrt{k^2+1} = (x - y\sqrt{k^2+1})(2k^2 + 1 + 2k\sqrt{k^2+1})$$
$$X_3 + K_3\sqrt{y^2+1} = (x + k\sqrt{y^2+1})(2y^2 + 1 + 2y\sqrt{y^2+1}).$$

(i) Taking norms gives $X_i^2 - (Y_i^2 + 1)K_i^2 = Y_i^2$.

(ii) $\gcd(X_i, Y_i) = \gcd(x, y)$ and $K_i > k$ for all i.

Generating the Type 1(a) solutions with g_0

Proposition. Type 1(a) solutions (k_n, x_n, y),

$$x_n + k_n\sqrt{D} = y(R + S\sqrt{D})^n, y \geq 2,$$

where $R = 2y^2 + 1, S = 2y, D = y^2 + 1$, can be expressed in terms of g_+ and g_0:

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

(ii) $(k_{n+1}, x_{n+1}, y) = g_0(k_n, x_n, y), n \geq 1$.

Generating the Type 1(b) solutions with g_0

Proposition. Type 1(b) solutions (k_n, x_n, y),

$$x_n + k_n\sqrt{D} = (y^2 + \epsilon y + 1 + (y+\epsilon)\sqrt{y^2+1})(R + S\sqrt{D})^n,$$

where $R = 2y^2 + 1, S = 2y, D = y^2 + 1$, and where $y \geq 1$ if $\epsilon = 1$ and $y \geq 2$ if $\epsilon = -1$, can be expressed in terms of g_+ and g_0:

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

(ii) $(k_{n+1}, x_{n+1}, y) = g_0(k_n, x_n, y), n \geq 1$.

Generating Type 2 exceptional solutions

Proposition.

(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 also Type 2 exceptional solution.

Jim White's forest of exceptional solutions

This is constructed recursively from the trivial solutions

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

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

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

First apply g_+ to each trivial solution, thereby producing a Type 1 exceptional solution. Then apply

$$g_+ \quad (\nearrow), \quad g_0 \quad (\longrightarrow), \quad g_- \quad (\searrow)$$

recursively to each exceptional solution. In each case, this produces a tree of exceptional solutions (k, x, y) in which $\gcd(x, y)$ is constant. The Type 1 solutions are coloured red.

Example: Root node type $(t, t, 0), t >= 2$

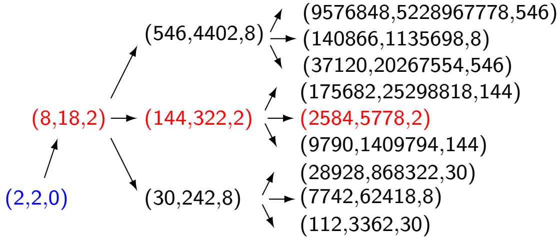


Figure: Tree fragment starting from $(t, t, 0) = (2, 2, 0)$.

Example: Root node type $(t, t^2 - t + 1, t - 1), t \geq 2$

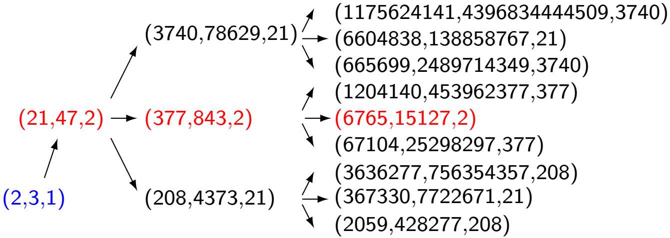


Figure: Tree fragment starting from $(t, t^2 - t + 1, t - 1) = (2, 3, 1)$.

Example: Root node type $(t, t^2 + t + 1, t + 1), t \geq 1$

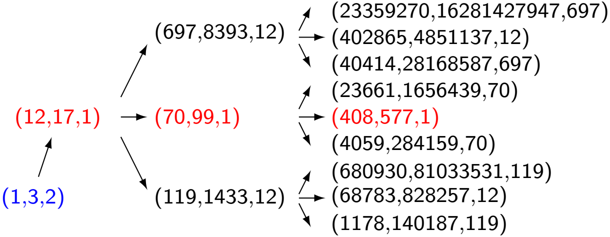
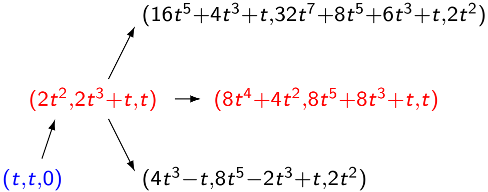


Figure: Tree fragment with root node $(t, t^2 + t + 1, t + 1) = (1, 3, 2)$.

Example: Tree fragment of $(k(t), x(t), y(t))$ starting from $(t, t, 0)$



Example: $(k(t), x(t), y(t))$ from $(t, t^2 + t + 1, t + 1)$

$$(t, t^2+t+1, t+1) \rightarrow (4t^3+4t^2+3t+1, 4t^4+4t^3+5t^2+3t+1, t)$$

$$(4t^3+4t^2+3t+1, 4t^4+4t^3+5t^2+3t+1, t) \rightarrow (k_1(t), x_1(t), y_1(t))$$

$$(4t^3+4t^2+3t+1, 4t^4+4t^3+5t^2+3t+1, t) \rightarrow (k_2(t), x_2(t), y_2(t))$$

$$(4t^3+4t^2+3t+1, 4t^4+4t^3+5t^2+3t+1, t) \rightarrow (k_3(t), x_3(t), y_3(t))$$

$$k_1(t) = 64t^7+128t^6+176t^5+160t^4+104t^3+48t^2+15t+2$$

$$x_1(t) = 256t^{10}+768t^9+1408t^8+1792t^7+1712t^6+1264t^5+732t^4+324t^3+109t^2+25t+3$$

$$y_1(t) = 4t^3+4t^2+3t+1$$

$$k_2(t) = 16t^5+16t^4+20t^3+12t^2+5t+1$$

$$x_2(t) = 16t^6+16t^5+28t^4+20t^3+13t^2+5t+1$$

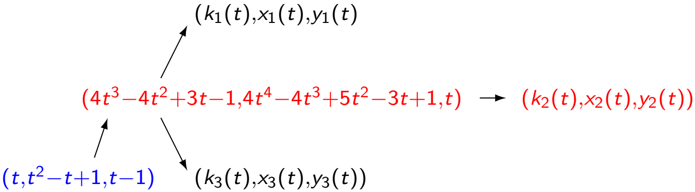
$$y_2(t) = t$$

$$k_3(t) = 16t^5+32t^4+36t^3+24t^2+9t+2$$

$$x_3(t) = 64t^8+192t^7+320t^6+352t^5+272t^4+152t^3+61t^2+17t+3$$

$$y_3(t) = 4t^3+4t^2+3t+1.$$

Example: $(k(t), x(t), y(t))$ from $(t, t^2 - t + 1, t - 1)$



$$
\begin{aligned}
k_1(t) &= 64t^7-128t^6+176t^5-160t^4+104t^3-48t^2+15t-2\\
x_1(t) &= 256t^{10}-768t^9+1408t^8-1792t^7+1712t^6-1264t^5+732t^4-324t^3+109t^2-25t+3\\
y_1(t) &= 4t^3-4t^2+3t-1\\
k_2(t) &= 16t^5-16t^4+20t^3-12t^2+5t-1\\
x_2(t) &= 16t^6-16t^5+28t^4-20t^3+13t^2-5t+1\\
y_2(t) &= t\\
k_3(t) &= 16t^5-32t^4+36t^3-24t^2+9t-2\\
x_3(t) &= 64t^8-192t^7+320t^6-352t^5+272t^4-152t^3+61t^2-17t+3\\
y_3(t) &= 4t^3-4t^2+3t-1.
\end{aligned}
$$

All exceptional solutions are in the forest

This follows from :

Lemma. Let $\mathscr{E}$ be the set of exceptional solutions (K, X, Y). Then with $T = RK - SX$, where $R = 2Y^2 + 1$ and $S = 2Y$,

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

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

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

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

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

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

All exceptional solutions are in the forest

The following function h takes an exceptional solution (K, X, Y) and either produces another exceptional solution (k, x, y) with $k < K$, or else creates a trivial solution.

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

Repeated application of h will eventually lead to a trivial solution.

The exceptional solutions are polynomials in t

It is clear that the exceptional solutions have the form $(K(t), X(t), Y(t))$, where the components are polynomials in t with integer coefficients, arising from the three types of root nodes:

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

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

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

Expressing x, y, k in terms of d, a, b, p, q

Theorem. Suppose (x, y) is a positive solution of Dujella's equation $x^2 - (k^2+1)y^2 = k^2$. Let $d = \gcd(x+k, x-k)$ and define positive integers a and b by

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

Then

$$(x+k)/da = p^2, \quad (x-k)/db = q^2,$$

where p and q are integers. Also

(i) $x = d(ap^2 + bq^2)/2, \quad y = dpq,$

(ii) $ap^2 - bq^2 = 2k/d, \quad \gcd(p, q) = 1,$

(iii) $ab = k^2 + 1, \quad \gcd(a, b) = 1,$

(v) k odd $\implies$ d even.

Restrictions on a, b and d for an exceptional solution

Proposition. If (k, x, y) is an exceptional solution and $d = \gcd(x + k, x - k)$, then

(i) $d \neq k, d \neq 2k$,

(ii) $a > 2, b > 2$.

p and q are small for an exceptional solution

Proposition. For an exceptional solution (k, x, y), p and q satisfy the following inequalities:

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

Hence $p < k$ and $q < k$.

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

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

Connections with continued fractions

Proposition. Consider the equation

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

where $a < b$, $D = ab = k^2 + 1$, $\gcd(a, b) = 1 = \gcd(p, q)$ and d divides $2k$. Let $(P_m + \sqrt{D})/Q_m$ denote the m–th complete quotient in the continued fraction expansion of $\sqrt{D}/a = \sqrt{b/a}$, with $P_0 = 0$ and $Q_0 = a$.

(i) If $d \geq 2$, then p/q is a convergent A_m/B_m of $\sqrt{b/a}$ and

$$Q_{m+1} = 2k/d.$$

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

$$|Q_m - Q_{m+1} + 2eP_{m+1}| = 2k.$$

Some properties of the continued fraction of $\sqrt{b/a}$

Proposition. Suppose $1 < a < b, \gcd(a,b) = 1, ab = k^2 + 1$. Then the continued fraction of $\sqrt{b/a}$ is periodic:

$$\sqrt{b/a} = [a_0, \overline{a_1, \ldots, a_{l-1}, 2a_0}].$$

and the period–length l is odd. Also

(i) $A_{l-1}/B_{l-1} = k/a$.

(ii) $A_{l-2}/B_{l-2} = (b - ka_0)/(k - aa_0)$.

(iii) $A_l/B_l = (b + ka_0)/(k + aa_0)$.

A parity conjecture

If $ap^2 - bq^2 = 2k$ has a primitive solution (p, q), where $D = ab = k^2 + 1$, k even, $\gcd(a, b) = 1$ and $2 < a < b$, then all Q_i are odd. Equivalently, using the identity

$$Q_i Q_{i-1} = D - P_i^2,$$

and the fact that if k is even, then D is odd, the conjecture is equivalent to the P_i being even. This in turn is equivalent to all partial quotients a_i being even, by virtue of the identity

$$P_{i+1} = a_i Q_i - P_i.$$

The unicity conjecture restated in terms of a family of diophantine equations

Conjecture. Consider the family of equations

$$ap^2 - bq^2 = \pm 2k/d, \qquad (1)$$

where d divides $2k$ (with d even if k is odd and $d \neq k, d \neq 2k$) and where $\gcd(a, b) = 1, D = ab = k^2 + 1, 2 < a < b$.

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

(ii) In the case of solubility, there is exactly one solution (p, q) with $dpq < k - 1$.

Example: $k = 8$

Here $D = k^2 + 1 = 65$ and only $(a, b, d) = (5, 13, 2)$ give solubility of $ap^2 - bq^2 = \pm 2k/d$ with $2 < a < b, ab = 65, \gcd(a, b) = 1$.

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	$(5 + \sqrt{65})/5$	$21/13$
6	1	$(5 + \sqrt{65})/8$	$29/18$

$$5A_0^2 - 13B_0^2 = (-1)^1 Q_1 = -8 = -2k/d$$
$$5A_3^2 - 13B_3^2 = (-1)^4 Q_4 = 8 = 2k/d.$$

Example $k = 8$ continued

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 unique exceptional solution of $x^2 - 65y^2 = 64$:

$$(x_0, y_0) = (d(ap_0^2 + bq_0^2)/2, dp_0 q_0) = (18, 2).$$

$k = 12$

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 $2 < a < b$, $ab = 145$, $\gcd(a, b) = 1$.

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	$(10 + \sqrt{145})/5$	$53/22$
4	2	$(10 + \sqrt{145})/9$	$118/49$

From the first period,

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

Example $k = 12$ continued

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 unique exceptional solution of $x^2 - 145y^2 = 144$:

$$(x_0, y_0) = (d(ap_0^2 + bq_0^2)/2, dp_0q_0) = (17, 1).$$

An example from the forest

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

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

$$d = \begin{cases} 1 & \text{if } t \text{ is odd} \\ 2 & \text{if } t \text{ is even,} \end{cases}$$

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

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

Forest example continued

(i) If t is even,

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

$$p/q = A_1/B_1, \text{ where } A_1 = 1, B_1 = t/2.$$

(ii) If t is odd,

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

$$p/q = (A_1 - A_0)/(B_1 - B_0), \text{ where } A_1 - A_0 = 1, B_1 - B_0 = t.$$

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

An example from deeper in the forest

$(k, x, y) = g_- g_- g_- g_+(t, t, 0), t \geq 2$. Then

$$(k, x, y) = (16t^5 - 12t^3 + t, 128t^9 - 160t^7 + 56t^5 - 4t^3 + t, 8t^4 - 4t^2)$$
$$(d, a, b) = (2t, 16t^4 - 4t^2 + 1, 16t^6 - 20t^4 + 5t^2 + 1)$$
$$(p, q) = (2t^2 - 1, 2t).$$

Also

$$\sqrt{b/a} = [t - 1, \overline{1, 2t - 2, 1, 2t - 1, 2t - 1, 1, 2t - 2, 1, 2t - 2}],$$

period length 9 and $Q_4 = 2k/d = 16t^4 - 12t^2 + 1, p/q = A_3/B_3$.

t	2	3	4	5	6
k	418	3567	15620	48505	121830

Some exact arithmetic BCmath programs

See
(i) http://www.numbertheory.org/php/dujella_test.html for a BCmath program which tests the unicity conjecture for a range of k using the continued fraction of $\sqrt{b/a}$.

(ii) http://www.numbertheory.org/php/exceptionalforest.html for a BCmath program which enables one to guess the continued fraction corresponding to an exceptional node $(k(t), x(t), y(t))$.

(iii) http://www.numbertheory.org/php/dujella_minus.html for a BCmath program which tests the unicity conjecture by considering the equivalent diophantine equation $X^2 - (k^2 + 1)y^2 = -k^2$.