AN EQUIVALENT FORM OF THE DUJELLA UNICITY CONJECTURE

The Dujella unicity conjecture states that the diophantine equation

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

has for $k > 1$ at most one positive integer solution (x, y) with $y < k - 1$. John Robertson has pointed out that this is equivalent to the statement that the diophantine equation

$$X^2 - (k^2+1)Y^2 = -k^2 \tag{2}$$

has at most one positive integer solution (X, Y) with $1 < Y < k$. In fact the equation

$$X + Y\sqrt{k^2+1} = (x + y\sqrt{k^2+1})(k - \sqrt{k^2+1}) \tag{3}$$

gives a 1–1 correspondence between the positive integer solutions (x, y) of (1) with $1 \leq y < k - 1$ and the positive solutions (X, Y) of (2) with $1 < Y < k$.

Proof. (John Robertson) Equation (3) is equivalent to

$$X = kx - (k^2+1)y \tag{4}$$

$$Y = x - ky. \tag{5}$$

or equivalently

$$x = (k^2+1)Y - kX \tag{6}$$

$$y = kY - X. \tag{7}$$

We consider the mapping $(x, y) \to (X, Y)$ which maps integer points satisfying (1) into integer points of (2), as is seen by taking norms in equation (3).

(i) (into): Assume $1 \leq x, 1 \leq y < k - 1$ and $x^2 - (k^2+1)y^2 = k^2$. Then $Y = x - ky > 1$. For clearly $Y > 0$. Also

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

so $Y = 1$ would imply $k - y = 1$, contradicting $y < k - 1$. Hence $Y > 1$. To see $Y < k$, write

$$x^2 - k^2y^2 = k^2 + y^2.$$

Then

$$Y = x - ky = \frac{k^2 + y^2}{x + ky} < \frac{2k^2}{2ky} = \frac{k}{2ky} \leq k.$$

Taking norms in equation (2) gives $X^2 - (k^2+1)Y^2 = -k^2$.

(ii) (onto): Now suppose $1 \leq X, 1 < Y < k$ and $X^2 - (k^2+1)Y^2 = -k^2$. Let x and y satisfy (4) and (5). Then $k^2Y^2 - X^2 = k^2 - Y^2 > 0$, so $y = kY - X > 0$. Also

$$y = kY - X = \frac{k^2 - Y^2}{kY + X} < \frac{k^2}{kY} = \frac{k}{Y} \leq \frac{k}{2} \leq k - 1.$$

(iii) (injectivity): this follows from (3).

□

LEMMA 0.1. *In the correspondence* (4) *and* (5), *we have* $Y < k/2, X < (k^2 + 1)/2$.

Then as $X < (k^2+1)/2 \iff Y^2 < (k^2+1)/4 + k^2/(k^2+1)$, it follows that $X < (k^2+1)/2$.

Proof.

$$\begin{aligned} Y < k/2 &\iff x - ky < k/2 \\ &\iff x < k(y + 1/2) \\ &\iff x^2 = (k^2+1)y^2 + k^2 < k^2(y^2 + y + 1/4) \\ &\iff 3k^2/4 < (k^2 - y)y. \end{aligned}$$

Then $1 \le y \le k-2$ implies

$$(k^2 - y)y \ge (k^2 - (k-2)) = k^2 - k + 2.$$

But

$$\begin{aligned} k^2 - k + 2 > 3k^2/4 &\iff k^2/4 > k - 2 \\ &\iff k^2 - 4k + 8 > 0 \\ &\iff (k-2)^2 + 4 > 0. \end{aligned}$$

Hence $(k^2 - y)y > 3k^2/4$ and consequently $Y < k/2$. □

THEOREM 0.1. *If* $k^2 + 1 = 2^\alpha p_1^{\beta_1} p_2^{\beta_2}$, *where* p_1 *and* p_2 *are distinct odd primes,* $1 \le \beta_1, \beta_2$, *then there is at most one positive solution* (X, Y) *of equation* (2) *such that* $1 < Y < k$.

Proof. The congruence $X^2 \equiv 1 \pmod{k^2+1}$ here has four solutions in the range $1 \le X < k^2 + 1$. Two of these are $X = 1$ and $X = k^2$. One of the other two solutions is in the range $1 < X < (k^2+1)/2$. □

REMARK 0.1. *If* $k^2 + 1 = 2p^a$ *or* p^a, *we see by the above congruence argument that there are no exceptional solutions. This was proved by A. Filipoi et. al. in* 2012.

See the link `http://www.numbertheory.org/php/dujella_minus.html` which solves the congruence $X^2 \equiv 1 \pmod{k^2+1}$ and finds the solutions (X, Y) of (2) and the corresponding solutions (x, y) of (1).