A Diophantine Definition of the Exponential Function

Martin Davis

We will work with the so-called Pell equation:

$$x^2 - dy^2 = 1 \text{ where } d = a^2 - 1 \text{ for some } a \geq 1 \quad (*)$$

We note the obvious solutions:

$$x = 1;\ y = 0$$

$$x = a;\ y = 1$$

The following lemmas investigate some of the rich properties of the solutions of (*).

Lemma 1. There are no integers x, y, positive, negative, or zero, satisfying (*) for which $1 < x+y\sqrt{d} < a+\sqrt{d}$.

Proof. Let x, y satisfy (*). Since

$$1 = (a + \sqrt{d})(a - \sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}),$$

the inequality implies (taking negative reciprocals)

$$-1 < -x + y\sqrt{d} < -a + \sqrt{d}.$$

Adding the inequalities $0 < 2y\sqrt{d} < 2\sqrt{d}$, that is, $0 < y < 1$, a contradiction.□

Lemma 2. Let x_1, y_1 and x_2, y_2 satisfy (*). Let

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}).$$

Then, x, y satisfies (*).

Proof. Replacing $\sqrt{d}$ by $-\sqrt{d}$ we get

$$x - y\sqrt{d} = (x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}).$$

Multiplying, we have

$$x^2 - dy^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = 1. \quad \square$$

Definition: We set $x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$.

Often we omit a just writing x_n, y_n.

Lemma 3. x_n, y_n satisfies (*).

Proof. Lemma 2 and mathematical induction.

Lemma 4. Let $x, y \geq 0$ satisfy (*). Then there is an n such that $x = x_n$ and $y = y_n$.

Proof. Since the sequence $(a + \sqrt{d})^n$ increases monotonically to infinity, there exists an n such that

$$(a + \sqrt{d})^n \leq x + y\sqrt{d} < (a + \sqrt{d})^{n+1}$$

If $(a+\sqrt{d})^n = x + y\sqrt{d}$, we are done. But otherwise

$$(a+\sqrt{d})^n < x + y\sqrt{d} < (a+\sqrt{d})^{n+1}$$

which would imply

$$1 < (a-\sqrt{d})^n(x + y\sqrt{d}) < a + \sqrt{d}$$

contradicting Lemmas 1 and 2. □

Lemma 5. $x_{m\pm n} = x_m x_n \pm d y_m y_n$ and $y_{m\pm n} = x_n y_m \pm x_m y_n$.

Proof.

$$\begin{aligned} x_{m+n} + y_{m+n}\sqrt{d} &= (a+\sqrt{d})^{m+n} \\ &= (a+\sqrt{d})^m (a+\sqrt{d})^n \\ &= (x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d}) \\ &= (x_m x_n + d y_m y_n) \\ &\qquad + (x_n y_m + x_m y_n)\sqrt{d} \end{aligned}$$

The $m - n$ case is handled similarly. □

Lemma 6. $x_{m\pm 1} = a x_m \pm d y_m$ and $y_{m\pm 1} = a y_m \pm x_m$.

Proof. Set $n = 1$ in Lemma 5. □

We are next going to study divisibility relationships among the y_n. We use the following standard notation:

$$\begin{array}{rl} r \mid s & \textit{for } s \text{ is divisible by } r \\ r \perp s & \textit{for the only common divisor} \\ & \quad \text{of } r \text{ and } s \text{ is } 1 \\ r \equiv s \pmod{m} & \textit{for } m \mid (r-s) \end{array}$$

Lemma 7. $x_n \perp y_n$.

Proof. Since $x_n^2 - dy_n^2 = 1$, any common divisor would divide 1. □

Lemma 8. If $n \mid m$ then $y_n \mid y_m$.

Proof. Let $m = nk$. The result is obvious for $k = 1$. By Lemma 5,

$$y_{n(s+1)} = x_n y_{ns} + x_{ns} y_n$$

Proceeding by induction, we may assume that y_{ns} is divisible by y_n. Hence the first term of the right side of this equation is divisible by y_n as well. Since the second term is obviously divisible by y_n, this gives the result. □

Lemma 9. $n \mid m$ if and only if $y_n \mid y_m$.

Proof. To prove the converse of Lemma 8, suppose that $y_n \mid y_m$ but it is not the case that $n \mid m$. So we can write

$m = qn + r,\ 0 < r < n$. Thus

$$y_m = y_{qn+r} = x_{qn}y_r + x_r y_{qn}$$

By Lemma 8, $y_n \mid y_{qn}$. Hence $y_n \mid x_{qn}y_r$. We will show that $y_n \perp x_{qn}$. Assuming this for the moment, we get $y_n \mid y_r$ which is impossible since $r < n$.

To complete the proof suppose that $s \mid y_n$ and $s \mid x_{nq}$. By Lemma 8, $s \mid y_{nq}$. By Lemma 7, this implies that $s = 1$. □

Lemma 10. $y_{nk} \equiv k x_n^{k-1} y_n \pmod{y_n^3}$.

Proof.

$$\begin{aligned} x_{nk} + y_{nk}\sqrt{d} &= (a + \sqrt{d})^{nk} \\ &= (x_n + y_n\sqrt{d})^k \\ &= \sum_{j=0}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{j/2} \end{aligned}$$

In this sum, the terms for which j is even contribute to x_{nk} while those with j odd contribute to y_{nk}, because it is these last that are an integer multiple of $\sqrt{d}$. Thus,

$$y_{nk} = k x_n^{k-1} y_n + \binom{k}{3} x_n^{k-3} y_n^3 d + \binom{k}{5} x_n^{k-5} y_n^5 d^2 + \dots$$

Thus the desired result follows. □

Lemma 11. $y_n^2 \mid y_{ny_n}$.

Proof. Setting $k = y_n$ in Lemma 10, we have:

$$y_{ny_n} = x_n^{y_n-1} y_n^2 + C y_n^3. \quad \square$$

Lemma 12. If $y_n^2 \mid y_m$ then $y_n \mid m$.

Proof. By Lemma 9, $n \mid m$; so let $m = nk$. By Lemma 10, $y_n^2 \mid k x_n^{k-1} y_n$, i.e., $y_n \mid k x_n^{k-1}$. But by Lemma 7, $y_n \perp x_n$. Hence, $y_n \mid k$. Finally, $y_n \mid m$. □

Lemma 13. $x_{n+1} = 2ax_n - x_{n-1}$ and $y_{n+1} = 2ay_n - y_{n-1}$.

Proof. By Lemma 6,

$$\begin{aligned} x_{n+1} &= ax_n + dy_n, \quad y_{n+1} = ay_n + x_n \\ x_{n-1} &= ax_n - dy_n, \quad y_{n+1} = ay_n - x_n \end{aligned}$$

Adding, we get $x_{n+1} + x_{n-1} = 2ax_n$ and $y_{n+1} + y_{n-1} = 2ay_n$. □

Lemma 14. $y_n(a) \equiv n \pmod{a-1}$.

Proof. This is obvious for $n = 0, 1$. Assuming the result known for $k-1$ and k, noting that $a \equiv 1 \pmod{a-1}$,

and using Lemma 13,

$$\begin{aligned} y_{k+1} &= 2ay_k - y_{k-1} \\ &\equiv 2k - (k-1) \pmod{a-1} \\ &= k+1 \quad \square \end{aligned}$$

Lemma 15. If $a \equiv b \pmod{c}$, then for all n, $x_n(a) \equiv x_n(b) \pmod{c}$ and $y_n(a) \equiv y_n(b) \pmod{c}$.

Proof. Use induction and Lemma 13. $\square$.

Lemma 16. When n is even y_n is even, and when n is odd y_n is odd.

Proof. Using Lemma 13,

$$y_{n+1} = 2ay_n - 2y_{n-1} + y_{n-1} \equiv y_{n-1} \pmod{2}.$$

Since $y_0 = 0$ and $y_1 = 1$, the result follows. $\square$

Lemma 17.

$x_n(a) - y_n(a)(a-y) \equiv y^n \pmod{2ay - y^2 - 1}$.

Proof. This is true for $n = 0, 1$, namely $x_0 - y_0(a-y) = 1$ and $x_1 - y_1(a-y) = y$. Assuming the result known for $k-1$ and k and using Lemma 13, we get

$$\begin{aligned}
x_{k+1} - y_{k+1}(a-y) &= [2ax_k - x_{k-1}] \\
&\quad -[2ay_k - y_{k-1}](a-y) \\
&= 2a[x_k - y_k(a-y)] \\
&\quad -[x_{k-1} - y_{k-1}(a-y)] \\
&\equiv 2ay^k - y^{k-1} \pmod{2ay - y^2 - 1} \\
&= y^{k-1}(2ay-1) \\
&\equiv y^{k-1}y^2 \pmod{2ay - y^2 - 1} \\
&= y^{k+1} \quad \square
\end{aligned}$$

Lemma 18. For all n, $y_{n+1} > y_n \geq n$.

Proof. Follows from Lemma 6. $\square$

Lemma 19. For all n,
$x_{n+1}(a) > x_n(a) \geq a^n$; $x_n(a) \leq (2a)^n$.

Proof. By Lemmas 6 and 13,
$ax_n(a) \leq x_{n+1}(a) \leq 2ax_n(a)$. The result follows by induction. $\square$

We write:

$$\lambda_k = \lambda_k(a) = y_{k+1}(a) + y_k(a);$$

$$\mu_k = \mu_k(a) = y_{k+1}(a) - y_k(a).$$

Lemma 20. $y_{2k+1} = \lambda_k \cdot \mu_k$.

Proof. Using Lemma 5,

$$\begin{aligned} y_{2k+1} &= x_k y_{k+1} + y_k x_{k+1} \\ 1 = y_1 &= x_k y_{k+1} - y_k x_{k+1}. \end{aligned}$$

Multiplying these equations:

$$\begin{aligned} y_{2k+1} &= x_k^2 y_{k+1}^2 - y_k^2 x_{k+1}^2 \\ &= (1 + dy_k^2) y_{k+1}^2 - y_k^2 (1 + dy_{k+1}^2) \\ &= y_{k+1}^2 - y_k^2 = \lambda_k \cdot \mu_k. \quad \square \end{aligned}$$

Lemma 21. $\lambda_k \perp \mu_k$.

Proof. By Lemmas 6 and 20, λ_k and μ_k are both odd. Let $s \mid \lambda_k$ and $s \mid \mu_k$. Then,

$$s \mid \lambda_k + \mu_k \text{ and } s \mid \lambda_k - \mu_k.$$

Thus, $s \mid 2y_{k+1}$ and $s \mid 2y_k$. Because s is odd, $s \mid y_{k+1}$ and $s \mid y_k$. By Lemma 6, $s \mid x_k$, and by Lemma 7, this implies $s = 1$. $\square$

Lemma 22. $(2s+1) \mid (2n+1)$ implies $\lambda_s \mid \lambda_n$ and $\mu_s \mid \mu_n$.

Proof. Let $(2n+1) = (2s+1)q$. Our proof is by induction on q. Of course the result is trivial if $q = 1$. Since q must be odd, it suffices to show that if the result is true for $q = q_1$, then it is also true for $q = q_1 + 2$. Let

$$\begin{aligned}(2n_1+1) &= (2s+1)q_1 \\ (2n+1) &= (2s+1)(q_1+2).\end{aligned}$$

Then, $n = n_1 + 2s + 1$. Using Lemma 5,

$$\begin{aligned}y_{n+1} \pm y_n &= y_{(n_1+1)+(2s+1)} \pm y_{n_1+2s+1} \\ &= (y_{n_1+1}x_{2s+1} + x_{n_1+1}y_{2s+1}) \\ &\quad \pm (y_{n_1}x_{2s+1} + x_{n_1}y_{2s+1}) \\ &= x_{2s+1}(y_{n_1+1} \pm y_{n_1}) + y_{2s+1}(x_{n_1+1} \pm x_{n_1}).\end{aligned}$$

The result follows using the induction hypothesis. □

Lemma 23. Let $(2n+1) = (2s+1)y_{2s+1}$. Then, $\lambda_s^2 \mid \lambda_n$ and $\mu_s^2 \mid \mu_n$. Also, $\lambda_s \perp \mu_n$ and $\mu_s \perp \lambda_n$.

Proof. By Lemma 11,

$$y_{2s+1}^2 \mid y_{2n+1}.$$

By Lemma 20,

$$\lambda_s^2 \mu_s^2 \mid \lambda_n \mu_n.$$

Lemma 22 implies that $\lambda_s \mid \lambda_n$ and $\mu_s \mid \mu_n$.

Now, suppose that $r \mid \lambda_s$ and $r \mid \mu_n$. Then also, $r \mid \lambda_n$. Thus, by Lemma 21, $r = 1$. We have shown that $\lambda_s \perp \mu_n$. Similarly, $\mu_s \perp \lambda_n$.

Since $\lambda_s^2 \mid \lambda_n \mu_n$ and $\lambda_s^2 \perp \mu_n$, we conclude that $\lambda_s^2 \mid \lambda_n$. Similarly, $\mu_s^2 \mid \mu_n$. $\square$

Lemma 24. We have the following modulo λ_k:

$$y_{2k+1} \equiv 0;\ x_{2k+1} \equiv 1;\ x_{k+1} \equiv x_k.$$

Proof. In this proof all congruences are modulo λ_k. The first relation follows at once from Lemma 20. Any divisor of λ_k and y_k must divide y_{k+1} and therefore also x_k. So, $\lambda_k \perp y_k$. Now, since $y_{k+1} \equiv -y_k$, we have:

$$\begin{aligned} 0 &\equiv y_{2k+1} = y_k x_{k+1} + x_k y_{k+1} \\ &\equiv y_k x_{k+1} - x_k y_k \\ &= y_k (x_{k+1} - x_k). \end{aligned}$$

Thus, $\lambda_k \mid (x_{k+1} - x_k)$, i.e. $x_{k+1} \equiv x_k$. It remains to

consider x_{2k+1}. But,

$$\begin{aligned} x_{2k+1} &= x_k x_{k+1} + d y_k y_{k+1} \\ &\equiv x_k^2 - d y_k^2 = 1. \ \square \end{aligned}$$

Lemma 25. (PERIODICITY) $y_{n+2k+1} \equiv y_n (\text{mod } \lambda_k)$.

Proof.

$$\begin{aligned} y_{n+2k+1} &= y_n x_{2k+1} + x_n y_{2k+1} \\ &\equiv y_n \cdot 1 + x_n \cdot 0 = y_n. \ \square \end{aligned}$$

Lemma 26. $y_{k+n} \equiv -y_{k+1-n} \pmod{\lambda_k}$.

Proof. Using Lemma 24,

$$\begin{aligned} y_{k+1-n} &= y_{k+1} x_n - x_{k+1} y_n \\ &\equiv -y_k x_n - x_k y_n \\ &= -y_{k+n}. \ \square \end{aligned}$$

Lemma 27. The numbers $\{y_i : 0 \leq i < 2k+1\}$, are mutually incongruent modulo λ_k.

Proof. By Lemma 18, $y_{k+1} \geq y_k + 1$. Therefore,

$$\lambda_k \geq 2y_k + 1.$$

That is,

$$y_k \leq (\lambda_k - 1)/2.$$

Since λ_k is an odd number, every integer is congruent modulo λ_k to one and only one of the numbers:

$$-(\lambda_k - 1)/2, \ldots, -1, 0, 1, \ldots, (\lambda_k - 1)/2.$$

Now,

$$0 = y_0 < y_1 < \ldots < y_k \leq (\lambda_k - 1)/2.$$

So the numbers $y_0, y_1, \ldots, y_k$ are certainly mutually incongruent. Furthermore, by Lemma 26, the numbers

$$y_{k+1}, y_{k+2}, \ldots, y_{2k}$$

are congruent respectively to:

$$-y_k, -y_{k-1}, \ldots, -y_1,$$

which gives the result. □

Theorem (THE MAIN LEMMA). Let $v \leq y_k(a)$, $m \equiv a \pmod{\lambda_k(a)}$, and $v \equiv y_n(m) \pmod{\lambda_k(a)}$. Then there is a $j \leq k$ such that $v = y_j(a)$ and $j \equiv n \pmod{2k+1}$.

Proof. By Lemma 15,

$$v \equiv y_n(m) \equiv y_n(a) \pmod{\lambda_k}.$$

Let $n = (2k+1)q + j,\ 0 \le j < 2k+1$. So,
$j \equiv n \pmod{2k+1}$. By Periodicity (Lemma 25),
$y_n(a) \equiv y_j(a) \pmod{\lambda_k}$. So,

$v \equiv y_j(a) \pmod{\lambda_k}$ and $v \le y_k(a) < x_k(a) + y_k(a) = \lambda_k$.

Now, $j \le k$, which we see as follows: If otherwise $j > k$, then using Lemma 26 with $n = j - k$, we would have

$$v \equiv y_j(a) \equiv -y_{2k+1-j}(a) \pmod{\lambda_k}.$$

But v and $-y_{2k+1-j}$ are different (one is non-negative and the other is negative) and both are included among the numbers (*) in the proof of Lemma 27; so this is impossible.
Now using $j \le k$ we have:

$$y_j(a) \le y_k(a) < \lambda_k.$$

Finally, we see that v and $y_j(a)$ are a pair of non-negative numbers, congruent modulo λ_k both $< \lambda_k$;
hence $v = y_j(a)$. $\square$

THE EQUATIONS

(I) $u + j = v$
(IIa) $p + (a-1)q = v + r + 1$
(IIb) $g = v + t + 1$
(III) $p^2 - (a^2-1)q^2 = 1$
(IVa) $h + (a+1)g = (b+1)(p + (a+1)q)^2$
(IVb) $h + (a-1)g = (c+1)(p + (a-1)q)^2$
(V) $h^2 - (a^2-1)g^2 = 1$
(VI) $m = (h + (a+1)g)z + a$
(VII) $m = (p + (a-1)q)f + 1$
(VIII) $x^2 - (a^2-1)y^2 = 1$
(IX) $y = d(p + (a-1)q) + u$
(X) $y = e(h + (a+1)g) + v$

(XI) $w^2 - (a^2-1)v^2 = 1$
(XII) $(w - v(a-\beta) - \alpha)^2 = \gamma^2(2a\beta - \beta^2 - 1)^2$
(XIII) $\alpha + \tau + 1 = 2a\beta - \beta^2 - 1$
(XIV) $\eta = \beta + \zeta + 1 = u + \xi + 1$
(XV) $a^2 - (\eta^2-1)(\eta-1)^2(\delta+1)^2 = 1$

Theorem. Equations (I) - (X) with parameters u, v, a have a solution for $a > 1$ if and only if $v = y_u(a)$.

Proof. First let (I) - (X) be satisfied. (III) and (V) permit us to write:

$$p = x_s(a), q = y_s(a); h = x_k(a), g = y_k(a).$$

Using Lemma 6,

$$\begin{aligned} p + (a-1)q &= x_s(a) + (a-1)y_s(a) \\ &= y_{s+1}(a) - y_s(a) = \mu_s(a);\ (*) \\ p + (a+1)q &= x_s(a) + (a+1)y_s(a) \\ &= y_{s+1}(a) + y_s(a) = \lambda_s(a);\ (*) \\ h + (a-1)g &= x_k(a) + (a-1)y_k(a) \\ &= y_{k+1}(a) - y_k(a) = \mu_k(a);\ (*) \\ h + (a+1)g &= x_k(a) + (a+1)y_k(a) \\ &= y_{k+1}(a) + y_k(a) = \lambda_k(a).\ (*) \end{aligned}$$

(I) and (IIa,b) yield the inequalities:

$$u \leq v < \mu_s, v < g = y_k(a).$$

Using (IVa,b), $\lambda_s^2 \mid \lambda_k,\ \mu_s^2 \mid \mu_k$. Therefore,

$$(y_{2s+1})^2 \mid y_{2k+1}.$$

By Lemma 12, $y_{2s+1} \mid 2k+1$. So, $\mu_s \mid 2k+1$.

(VI) and (VII) give us the congruences:

$$m \equiv a \pmod{\lambda_k}, m \equiv 1 \pmod{\mu_s},$$

and (IX) and (X) yield the congruences:

$$y \equiv u \pmod{\mu_s}, y \equiv v \pmod{\lambda_k}.$$

Finally, by (VIII), there is a number n such that $y = y_n(m)$. Therefore, we can apply the main lemma to obtain a number $j \leq k$ such that

$$v = y_j(a) \text{ and } n \equiv j \pmod{2k+1}.$$

It remains to show that $j = u$. Since $\mu_s \mid 2k+1$, we have

$$n \equiv j \pmod{\mu_s}.$$

Since $m \equiv 1 \pmod{\mu_s}$, Lemma 14 tells us that $y_n(m) \equiv n \pmod{\mu_s}$. Thus,

$$u \equiv y \equiv n \equiv j \pmod{\mu_s}.$$

To show that $u = j$ it will therefore suffice to show that they are both $< \mu_s$. But we already know that $u < \mu_s$. And, using Lemma 18,

$$j \leq y_j(a) = v < \mu_s.$$

We conclude that $v = y_u(a)$.

Conversely, let $v = y_u(a)$. We proceed to show how to satisfy (I)-(X). Since Lemma 18 implies that $v \geq u$, we can choose j to satisfy (I). Choose s so large that $y_s(a) > v$, and set $p = x_s(a), q = y_s(a)$, thus satisfying (III). Then,

$$p + (a-1)q \geq y_s(a) > v$$

so (IIa) can be satisfied. Let k be the integer satisfying the equation:

$$(2k+1) = y_{2s+1}(2s+1),$$

and set $h = x_k(a), g = y_k(a)$, thus satisfying (V). Then,

$$g = y_k(a) \geq y_s(a) = q > v.$$

So (IIb) is satisfiable. The relations (*) hold, and by Lemma 23,

$$\lambda_s^2 \mid \lambda_k,\ \mu_s^2 \mid \mu_k, \text{ and } \mu_s \perp \lambda_k.$$

Thus, (IVa,b) can be satisfied, and, by the Chinese Remainder Theorem, there is a number m such that

$$m \equiv 1 \pmod{\mu_s},\ m \equiv a \pmod{\lambda_k}.$$

Therefore, we can satisfy (VI) and (VII). Letting $x = x_u(m), y = y_u(m)$, (VIII) is satisfied. Using Lemma 15,

$$y = y_u(m) \equiv y_u(a) = v \pmod{\lambda_k}.$$

Hence, (X) can be satisfied. Finally, by Lemma 14,

$$y = y_u(m) \equiv u \pmod{m-1},$$

so $y \equiv u \pmod{\mu_s}$, and we can satisfy (X). □

Lemma 28. If $a > y^n$ and $y \geq 1$, then $2ay - y^2 - 1 > y^n$.

Proof. Set $g(y) = 2ay - y^2 - 1$. Then, $g(1) = 2a - 2 \geq a$, since $a > 1$. Also, $g'(y) = 2a - 2y > 0$ for $y < a$. So g(y) is increasing in the interval $1 \leq y < a$, and therefore, for such y,

$$g(y) \geq g(1) \geq a.$$

Finally, assuming that $a > y^n \geq y \geq 1$, we have:

$$g(y) \geq a > y^n.$$

Theorem. Let $\beta \geq 1$. Then equations (I) - (XV) with parameters α, β, u, are satisfiable if and only if $\alpha = \beta^u$.

Proof. First, let (I) - (XV) be satisfied. By (XV), $a > 1$. Then, by the previous theorem, $v = y_u(a)$. By (XI),

$w = x_u(a)$. (XII) yields the congruence:

$$\alpha \equiv x_u(a) - y_u(a)(a - \beta) \pmod{2a\beta - \beta^2 - 1}.$$

So, by Lemma 17,

$$\alpha \equiv \beta^u \pmod{2a\beta - \beta^2 - 1}.$$

We use the, by now familiar, device of converting this congruence into an equation, by showing that both sides are less than the modulus. In fact, by (XIII), $\alpha < 2a\beta - \beta^2 - 1$. Now, (XIV) implies $\beta, u < \eta$. By (XV), there is an n such that

$$a = x_n(\eta), (\eta - 1)(\delta + 1) = y_n(\eta).$$

By Lemma 14, $n \equiv (\eta - 1)(\delta + 1) \pmod{(\eta - 1)}$, i.e. $(\eta - 1) \mid n$. Since $n \neq 0$ (else $a = 1$), $n \geq \eta - 1$. So, by Lemma 19,

$$a = x_n(\eta) \geq \eta^n \geq \eta^{\eta - 1} > \beta^u.$$

Since, $\beta \geq 1$, Lemma 28 implies that $\beta^u < 2a\beta - \beta^2 - 1$. Hence, $\alpha = \beta^u$.

Conversely, let $\alpha = \beta^u$, and let us satisfy (I) - (XV). Choose $\eta > \beta, u$, thus satisfying (XIV), and let

$a = x_{\eta-1}(\eta)$. Then,

$$y_{\eta-1}(\eta) \equiv \eta - 1 \equiv 0 \pmod{\eta - 1}.$$

Hence, we can write $y_{\eta-1}(\eta) = (\eta - 1)(\delta + 1)$, thus satisfying (XV). Since, $\beta \geq 1$, Lemma 28 enables us to find τ satisfying (XIII). Let $w = x_u(a), v = y_u(a)$ so (XI) is satisfied, and by the previous theorem, (I) - (X) are satisfied. Using Lemma 17, we have the congruence:

$$\alpha \equiv w - v(a - \beta) \pmod{2a\beta - \beta^2 - 1},$$

and so we can find γ satisfying (XII). □

Finally, we obtain our goal:

Theorem. The predicate $\alpha = \beta^u$ is Diophantine.

Proof. By summing the squares of (I) - (XV) we obtain a polynomial $p(\alpha, \beta, u, z_1, z_2, \ldots, z_n)$ which takes on no negative values such that for $\beta \neq 0$,

$$\alpha = \beta^u \leftrightarrow (\exists z_1, z_2, \ldots, z_n)[p(\alpha, \beta, u, z_1, z_2, \ldots, z_n) = 0].$$

To deal with the $\beta = 0$ case, recall that $0^u = 0$ when $u \neq 0$ and $0^0 = 1$. Hence, for any α, β, u, the condition $\alpha = \beta^u$ is equivalent to the solvability of the equation:

$$[(\beta - t - 1)^2 + p(\alpha, \beta, u, z_1, \ldots, z_n)]$$
$$\cdot[(\alpha - 1)^2 + \beta^2 + u^2] \cdot [\alpha^2 + \beta^2 + (u - t - 1)^2] = 0.$$

This gives the result. $\square$