Now we can prove CL #1 : i.e.

$$y(a,k) \equiv y(a,\ell) \bmod x(a,M)$$
$$\Rightarrow$$
$$k \equiv \pm \ell \bmod 2M$$

Pf:- Sps $y(a,k) \equiv y(a,\ell) \bmod x(a,M)$

- By Subdemma (II.2), may assume $1 \le k, \ell \le 4M$
- if $k, \ell \le M$ then by subdemma(I.) we have $y(a,k), y(a,\ell) \le \frac{x(a,M)}{2}$ so actually $y(a,k) = y(a,\ell)$ which implies $k = \ell$
- in general case, observe for any $k \in [0,4M]$ at least one of the numbers $\varepsilon_0 2M + \varepsilon_1 k$ is in $[0,M]$

(not quite true: for $k \in [3M,4M]$ need $2(2M) - k$ but $y(4M-k) \equiv y(-k) = -y(k)$ so ok in this case too)

- since $y(a,k) = \pm y(a, \varepsilon_0 2M + \varepsilon_1 k)$ so then invoking subdemma I again as above gives desired conclusion ✓

We turn now to

Crucial lemma #2: $y^2(a,i) \mid y(a,j)$
$\Rightarrow y(a,i) \mid j$

Pf: Sps $y^2(a,i) \mid y(a,j)$
Since y's increasing we have $i \le j$
Write $j = iq + r$ w/ $r < i$
Two cases

Case 1: $r = 0$
then $x(a,j) + \sqrt{a^2-1}\, y(a,j) =$
$(x(a,i) + \sqrt{a^2-1}\, y(a,i))^q$

So then:
$$y(a,j) = \sum_{\ell \le q \text{ odd}} x(a,i)^{q-\ell} y(a,i)^\ell (a^2-1)^{\ell-1/2} \binom{q}{\ell}$$
$$\equiv x_{(a,i)}^{q-1} y(a,i) q \pmod{y^2(a,i)}$$
$$\equiv 0 \text{ by hypothesis}$$

Hence $y^2(a,i) \mid x_{(a,i)}^{q-1} y(a,i) q$
$\Rightarrow y(a,i) \mid x_{(a,i)}^{q-1} q$

but $x(a,i), y(a,i)$ coprime since sol'n to Pell's (recall Bezout's Lemma!)
$\Rightarrow y(a,i) \mid q$
$\Rightarrow y(a,i) \mid j$ ✓

Case 2: $r \neq 0$

then $x(a,j) + \sqrt{a^2-1}\, y(a,j) =$

$$(x(a,i) + \sqrt{a^2-1}\, y(a,i))^q (x(a,r) + \sqrt{a^2-1}\, y(a,r))$$

$=$

$$\Big[\sum_{e=1,\text{even}} x(a,i)^{q-e}\, y(a,i)^e\, (a^2-1)^{e/2} \binom{q}{e}$$

$$+ \sum_{e=1,\text{odd}} x(a,i)^{q-e}\, y(a,i)^e\, (a^2-1)^{e-1/2} \sqrt{a^2-1} \binom{q}{e} \Big]$$

$$\times \left(x(a,r) + \sqrt{a^2-1}\, y(a,r)\right)$$

So that

$$y(a,j) = y(a,r) \Sigma(\cdots) + x(a,r) \Sigma(\cdots)$$

(w/o $\sqrt{a^2-1}$)

$$\equiv y(a,r)\, x(a,i)^q + x(a,r)\, x(a,i)^{q-1} y(a,i) q$$

$$\pmod{y^2(a,i)}$$

$$\equiv 0 \quad \text{by hyp.}$$

hence $y^2(a,i)$	expression above
hence $y^2(a,i)$	" "
hence $y(a,i)$	$y(a,r)\, x(a,i)^q$
hence $y(a,i)$	$y(a,r)$

since coprime to $x(a,i)^q$

Contradiction, as $r < i$ ✓

We can finally formulate a Diophantine definition to $y(a,n)$ using Lemmas

Theorem For $n>1$, $a>2$ we have:
$y = y(a,n)$ iff $\exists x, X_2, Y_2, A, Z, W$ s.t.

① $x^2-(a^2-1)y^2 = 1$ and $y>n$ and $y \equiv n \pmod{a-1}$
② $X_2^2-(A^2-1)Y_2^2 = 1$ and $Y_2 \equiv n \pmod{A-1}$
③ $A \equiv a \pmod{Z}$
④ $Y_2 \equiv y \pmod{Z}$
⑤ $Z^2-(a^2-1)W^2 = 1$
⑥ $A \equiv 1 \pmod{2y}$
⑦ $W \equiv 0 \pmod{y^2}$

(notice: this is Dio, and if we like we can derive $n=0,1$ $a=0,1,2$ cases separately to get full Dio defn for $y(a,n)$)

Pf: ($\Rightarrow$) Assume $y = y(a,n)$
must show $\exists x, X_2, Y_2, Z, A, W$ as above

Let $x = x(a,n)$ then indeed $y>n$ (for $n=1$ $y = a^2-1 > 1$ and strictly increasing) and we prove $y \equiv n \pmod{a-1}$, so ① holds.

Define $X_2 = x(A,n)$ $Y_2 = y(A,n)$
where $A = a + Z^2(Z^2 - a)$

Haven't defined Z but once we do
we'll have ② (X_2, Y_2 solve Pell's)
and also ③ clearly.

We get ④ too, from the following:

General observation: if $b \equiv c \pmod d$
then $y(b,k) \equiv y(c,k) \pmod d$

Pf: $y(\alpha,k)$ is a polynomial in α w/
integer coefficients. ✓

So ④ follows from ③

Soneed to define Z, W so ⑤-⑦ hold.
⑤ is just Pell's. To get a sol'n
satisfying 6,7 enough to arrange
$W \equiv 0 \pmod{2y^2}$
this gives ⑦ immediately, i.e. $W \equiv 0 \pmod{y}$
and also, by ⑤ gives $Z^2 \equiv 1 \pmod{2y}$
So that by def'n of A we get
$A \equiv 1 \pmod{2y}$, giving ⑥

How to get such z w?

As before for any M, k we have

$$x(a,kM) + \sqrt{a^2-1}\, y(a,kM) = (x(a,M) + \sqrt{a^2-1}\, y(a,M))^k$$

$$\Rightarrow y(a,kM) = \sum_{i \le k \text{ odd}} x(a,M)^{k-i} y(a,M)^i (a^2-1)^{\frac{i-1}{2}} \binom{k}{i}$$

$$\equiv k x(a,M)^{k-1} y(a,M) \pmod{y^3(a,M)}$$

Let $k = 2y = 2y(a,n)$ and let $M = n$

then let $w = y(a, 2ny)$ $z = x(a, 2ny)$

Get ⑤ for free

Observe $w \equiv 2y x^{k-1} y \pmod{y^3}$

$\equiv 2y^2 x^{k-1}$ ⑧

So $w = 2y^2 x^{k-1}$ + remaining terms of sum each div's by y^3

Clearly $y^2 \mid w$

If y is even then $2y^2 \mid w$

If y is odd then still $w = y(a, 2ny)$ is even, since by an easy

Induction the even terms $y(a, 2(\dots))$ are always even. So W divisible by both 2 and y^2 in this case too, and so by $2y^2$.

↪ in all cases $W \equiv 0 \pmod{2y^2}$ ✓

($\Leftarrow$) Assume we have x, X_2, Y_2, A, Z, W and y, n as in (1)–(7)

Since x, y solve Pell's by ① we know $y = y(a, N)$ for some N. Need to show $N = n$.

By our previous Lemma we know $y \equiv N \pmod{a-1}$ and hence $N \equiv n \pmod{a-1}$ by ①.

By ② we know $Y_2 = y(A, N_2)$ for some N_2 and so by second clause of ② and Lemma we get $N_2 \equiv n \pmod{A-1}$

By ⑤ we know $Z = x(a, M)$ $W = y(a, M)$ for some M.

Now, as $y(a, n)$ is a polynomial in a w/ integer coefficients by ③ and ④ we know:

$$y(A, N_2) \equiv y(a, N_2) \equiv y(a, N) \pmod{2}$$

By CL #1 we have $N_2 = \pm N \pmod{2M}$

By CL #2 and ⑦ we have $y(a,N) \mid M$ and hence $2y \mid 2M$, which as previously we gave

$$N_2 = \pm N \pmod{2y}$$

On the other hand, since $N_2 \equiv n \pmod{A-1}$ by above and by ⑥ we have $A \equiv 1 \pmod{2y}$ (so $2y \mid A-1$)

we get:

$$N_2 \equiv n \pmod{2y}$$

but $N < y$ since $y = y(a,N)$ and by ① we knew $n < y$.

So $N_2 \equiv \pm N \pmod{2y} \Rightarrow N_2 = N$
and $N_2 \equiv n \pmod{2y} \Rightarrow N_2 = n$

$\Rightarrow n = N$ ✓