9.4 EXPONENTIATION

In this section we show that the function m^n is diophantine, thus completing the proof of the main theorem. We have to begin by considering the behaviour of the solutions to some difference equations.

Let a be an integer greater than 1. Define x_n and y_n by

$$x_{n+1} = 2ax_n - x_{n-1}, \quad x_0 = 1, \quad x_1 = a,$$
$$y_{n+1} = 2ay_n - y_{n-1}, \quad y_0 = 1, \quad y_1 = 1.$$

When the parameter a needs consideration we refer to these as $x_n(a)$ and $y_n(a)$.

Let $d = a^2 - 1$; then $\sqrt{d}$ is irrational. It follows that if $m + n\sqrt{d} = u + v\sqrt{d}$ then $m = u$ and $n = v$, and so we also have $m - n\sqrt{d} = u - v\sqrt{d}$.

(I) It is easy to see, by induction, that $x_n \pm y_n\sqrt{d} = (a \pm \sqrt{d})^n$. Since $(a+\sqrt{d})(a-\sqrt{d}) = 1$, we also have that $x_n - y_n\sqrt{d} = (a+\sqrt{d})^{-n}$. Hence $x_n^2 - dy_n^2 = 1$.

(II) Conversely, we show that any solution of $x^2 - dy^2 = 1$ with x and y in $\mathbf{N}$ must satisfy $x = x_n$ and $y = y_n$ for some n. Observe first that there must be some n with $(a+\sqrt{d})^n \leq x + y\sqrt{d} < (a+\sqrt{d})^{n+1}$. Let $u + v\sqrt{d}$ be $(x+y\sqrt{d})(a-\sqrt{d})^n$, so both u and v are integers. We also have $u - v\sqrt{d} = (x-y\sqrt{d})(a+\sqrt{d})^n$, and so $u^2 - dv^2 = x^2 - dy^2 = 1$.

Since $(a-\sqrt{d})^n = (a+\sqrt{d})^{-n}$, we have $1 \leq u + v\sqrt{d} < a + \sqrt{d}$. Taking the inverse of these inequalities and changing sign, we find that $-1 \leq -u + v\sqrt{d} < -a + \sqrt{d}$. Adding these to the original inequalities then gives $0 \leq 2v\sqrt{d} < 2\sqrt{d}$. Hence $v = 0$, and so $u = 1$, since $u^2 - dv^2 = 1$. It follows that $x + y\sqrt{d} = (a+\sqrt{d})^n$, so $x = x_n$ and $y = y_n$, as required.

(III) It follows easily from the equalities $x_n \pm y_n\sqrt{d} = (a \pm \sqrt{d})^n = (a+\sqrt{d})^{\pm n}$ that $x_{m\pm n} + y_{m\pm n}\sqrt{d} = (x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d})$, and hence that we have the addition formulas $x_{m\pm n} = x_m x_n \pm dy_m y_n$, and $y_{m\pm n} = x_n y_m \pm x_m y_n$. In particular $x_{n\pm 1} = ax_m \pm dy_m$, $y_{m\pm 1} = ay_m \pm x_m$. It follows that $y_{m+1} > y_m$, and hence that $y_m \geq m$ for all m.

(IV) We denote the greatest common divisor of two integers r and s by (r,s). Since $x_n^2 - dy_n^2 = 1$, we see that $(x_n, y_n) = 1$. By induction on k, using the addition formulas, we see that $y_n | y_{nk}$ for all n and k, where $r|s$ means that r divides s.

(V) We can now deduce the $y_n|y_t$ iff $n|t$. The previous remark gives the result if $n|t$. Assume that $y_n|y_t$ and that n does not divide t. Write t as $nq + r$, where $0 < r < n$. Since $y_t = x_r y_{nq} + x_{nq} y_r$, and we already know that y_n divides $y_n q$, we see that $y_n | x_{nq} y_r$. As $(y_{nq}, x_{nq}) = 1$, and $y_n | y_{nq}$, it follows that $y_n | y_r$. But we know that $y_r < y_n$, a contradiction.

(VI) We next show that $y_{nk} \equiv kx_n^{k-1} y_n \bmod y_n^3$. To see this, we write $x_{nk} + y_{nk}\sqrt{d}$ as $(x_n + y_n\sqrt{d})^k$. Expanding this by the binomial theorem, and equating the terms involving $\sqrt{d}$ gives the result.

(VII) It follows immediately that if $k = y_n$ then $y_n^2 | y_{nk}$. As a partial converse to this we show that $y_n|t$ if $y_n^2|y_t$. We already know that $n|t$, since $y_n|y_t$. Write t as nk. Then we know that y_n^2 must divide $kx_n^{k-1}y_n$, so that y_n divides kx_n^{k-1}. Since $(y_n, x_n) = 1$, this tells us that y_n divides k.

(VIII) From the difference equation, easy inductions (the initial cases when n is 0 or 1 being obvious) give the following results. $y_n \equiv n \bmod 2$, and $y_n \equiv n \bmod (a-1)$. Also if $a \equiv b \bmod c$ we find that, mod c, $x_n(a) \equiv x_n(b)$ and $y_n(a) \equiv y_n(b)$.

(IX) We now show that $x_{2n\pm j} \equiv -x_j \bmod x_n$, and hence $x_{4n\pm j} \equiv x_j \bmod x_n$. For the addition formula tells us that $x_{2n\pm j} \equiv x_n x_{n\pm j} + dy_n y_{n\pm j} \equiv dy_n(y_n x_j \pm x_n y_j) \equiv dy_n^2 x_j \equiv (x_n^2 - 1)x_j \equiv -x_j$.

(X) The most difficult of our results, is the following. Let $x_i \equiv x_j \bmod x_n$, with $i \leq j \leq 2n$ and $n > 0$. Then $i = j$, unless $a = 2$, $n = 1$, $i = 0$, and $j = 2$.

We first suppose that x_n is odd, and let $q = (x_n - 1)/2$. Then no two of the numbers $-q, \ldots, q$ are congruent mod x_n, and every integer is congruent to one of them. Now we know that $1 = x_0 < x_1 < \ldots < x_{n-1}$, and that $x_{n-1} \leq x_n/a \leq x_n/2$. In particular $x_{n-1} \leq q$. Also we know that the numbers $x_{n+1}, \ldots, x_{2n}$ are congruent mod x_n to $-x_{n-1}, \ldots, -x_0$, by the previous result. Hence the numbers $x_0, \ldots, x_{2n}$ are mutually incongruent mod x_n.

When x_n is even, we let q be $x_n/2$. In this case $-q \equiv q \bmod x_n$. The result will follow as before unless $x_{n-1} = q$; this possiblity would give $x_{n+1} = -q$. However this case requires $x_n = 2x_{n-1}$, and, as we know that $x_n = ax_{n-1} + dy_{n-1}$, we must have $a = 2$ and $y_{n-1} = 0$, so that $n = 1$, as needed.

The previous result can be extended to show that if $x_j \equiv d_i \bmod x_n$, with $0 < i \leq n$ and $0 \leq j < 4n$, then either $j = i$ or $j = 4n - i$. For if $j \leq 2n$, we get $i = j$ unless we are in the exceptional case. Since i is not 0, we would then have $i = 2$, $j = 0$, and $n = 1$, contradicting $i \leq n$, so this case cannot happen. If $j > 2n$ define k as $4n - j$. Then $k > 0$, and $x_k = x_j = x_i \bmod x_n$. As $0 < k < 2n$, we cannot be in the exceptional case, and so must have $k = i$.

It follows at once that if $0 < i \leq n$ and $x_i \equiv x_j \bmod x_n$ then $j \equiv \pm i \bmod 4n$. For we need only write j as $4nq + k$, where $0 \leq k < 4n$ and use the previous result and the fact that $x_{4n+r} \equiv x_r$ for all r.

We are now in a position to prove the main results.

Proposition 9.9 *The function $y_k(a)$ is diophantine.*

Proof We show that, provided k is non-zero (the general case can be obtained from this, but is not needed) $y = y_k(a)$ iff $a > 1$ (else $y_k(a)$ is not defined) and there are positive integers $x, u, v, s, t, b, r, p, q, c$, and d satisfying the following eight equations.

$$x^2 - (a^2 - 1)y^2 = 1 \tag{1}$$
$$u^2 - (a^2 - 1)v^2 = 1 \tag{2}$$
$$s^2 - (b^2 - 1)t^2 = 1 \tag{3}$$
$$v = ry^2 \tag{4}$$
$$b = 1 + 4py = a + qu \tag{5}$$
$$s = x + cu \tag{6}$$
$$t = k + 4(d - 1)y \tag{7}$$
$$y \geq k. \tag{8}$$

First suppose the equations have a solution. As the variables are not zero, there will, by (II), be a positive i, j, and n such that $x = x_i(a)$, $y = y_i(a)$, $u = x_n(a)$, $v = y_n(a)$, $s = x_j(b)$, and $t = y_i(b)$. By (4), $y \leq v$, and so $i \leq n$. Form (5), $b \equiv a \bmod x_n(a)$, from which we know, by (VII), that $x_j(b) \equiv x_j(a) \bmod x_n(a)$. From (t) we have $x_j(b) \equiv x_i(a) \bmod x_n(a)$. Hence we have $x_j(a) \equiv x_i(a) \bmod x_n(a)$, so (X) tells us that $j \equiv \pm i \bmod 4n$.

Equation (4) tells us that $y_i(a)^2 | y_n(a)$, from which we know that $y_i(a) | n$. Hence $j \equiv \pm i \bmod 4y_i(a)$.

We know that $y_j(b) \equiv j \bmod (b - 1)$. By (5), $b \equiv 1 \bmod 4y_i(a)$, so that $y_j(b) \equiv j \bmod 4y_i(a)$. By (7), we have $y_j(b) \equiv k \bmod 4y_i(a)$. Consequently $k \equiv \pm i \bmod 4y_i(a)$.

However, we know that $i \leq y_i(a)$, and condition (8) tells us that $k \leq y_i(a)$. The congruence then requires that $i = k$. As i is defined to satisfy $y = y_i(a)$, we have, as required, $y = y_k(a)$.

Conversely, suppose that $y = y_k(a)$. Set x to be $x_k(a)$, so that (1) holds. Let $m = 2ky_k(a)$, and define $u = x_m(a)$, $v = y_m(a)$. Then (2) holds. We find that $y^2 | v$, since we have that $y^2 | y_{m/2}(a)$, and the latter divides $y_m(a)$. Hence we can find r satisfying (4). Since m is even, we know from (VIII) that v is even, and hence u is odd.

As u is odd and $(u, v) = 1$, adn y divides v, we find that $(u, 4y) = 1$. By the Chinese Remainder Theorem (Theorem 9.11 below) there is a non-negative b_0 satisfying $b_0 \equiv 1 \bmod 4y$ and $b_0 \equiv a \bmod u$. Adding a suitable multiple of $4uy$ to b_0, we can find positive b, p and q satisfying (5). Then (3) is satisfied by putting s and t to be $x_k(b)$ and $y_k(b)$.

Since $b > a$, we have $s > x$, as $s = x_k(b)$ and $x = x_k(a)$. It also follows, since $b \equiv a \bmod u$, that $s \equiv x \bmod u$. Hence we can choose c to satisfy (6).

Since t is $y_k(b)$, we know that $t \geq k$ and $t \equiv k \bmod (b - 1)$. By (5) we have that $t \equiv k \bmod 4y$, so that (7) can be satisfied. Finally (8) holds, since $y = y_k(a)$. •

Theorem 9.10 *The function a^n is diophantine.*

Proof It is most convenient to assume that $n > 0$ and $a > 1$. We do not need the general case; it can be obtained by a simple modification.

We define Near(u, v) to be the nearest integer to v/u. The function Near is diophantine, since Near(u, v) $= w$ iff $(2\mathrm{rem}(u, v) \leq u \wedge w = \mathrm{quo}(u, v)) \vee (2\mathrm{rem}(u, v) > u \wedge w = \mathrm{quo}(u, v) + 1)$.

We shall show that $a^n = Near(y_{n+1}(k), y_{n+1}(ka))$ provided k is large enough. By the previous proposition, a^n will be diophantine if the requirement that k is large enough can be expressed as a diophantine condition.

It is ease to check, by induction, that, for any $b > 1$ and any n, $(2b-1)^n \leq y_{n+1}(b) \leq (2b)^n$. Apply this for $b = ka$ and for $b = k$, and divide the inequalities. We find that $y_{n+1}(ka)/y_{n+1}(k)$ lies between $(2ka-1)^n/(2k)^n = a^n(1-1/2ka)^n$ and $(2ka)^n/(2k-1)^n = a^n(1-1/2k)^{-n}$. Hence $Near(y_{n+1}(k), y_{n+1}(ka)) = a^n$ if $(1-1/2ka)^n > 1 - 1/2a^n$ and $(1-1/2k)^- n < 1 + 1/2a^n$.

Since $y_{n+1}(a) \geq (2a-1)^n > a^n$, it is enough to require that $(1-1/2ka)^n > 1 - 1/2y_{n+1}(a)$ and $(1-1/2k)^{-n} < 1 + 1/2y_{n+1}(a)$, and the latter condition can be written as $(1-1/2k)^n > (1+1/2y_{n+1}(a))^{-1}$.

Now $(1-x)^n > 1 - nx$ for any real x between 0 and 1 (because $(1-x)^n + nx$ ahs a positive derivative). Hence the required conditions hold provided that $1 - n/2ka > 1 - 1/2y_{n+1}(a)$ and $1 - n/2k > (1 + 1/2y_{n+1}(a))^{-1}$. These two conditions, when cleared of fractions, are diophantine conditions, since $y_{n+1}(a)$ is diophantine. •