Problem 6: Miller — Rabin revisited

If n is prime, then we have $\varphi(n) = n - 1$ => $\varphi(n) = 2^k 3^l m$
and $a^{\varphi(n)} = 1 \ mod \ n$

$$a^{2^k 3^l m} = 1 \ (mod \ n)$$

=> $$a^{2^k 3^l m} - 1 = 0 \ (mod \ n) \qquad (1)$$

Let $d = 3^l m$,
Based on Miller - Rabin primality test, we expand the left side of equation (1)

$$a^{2^k d} - 1$$
$$= (a^{2^{k-1}d} - 1)(a^{2^{k-1}d} + 1)$$
$$= (a^{2^{k-2}d} - 1)(a^{2^{k-2}d} + 1)(a^{2^{k-1}d} + 1)$$
$$= (a^{2^{k-k}d} - 1)(a^{2^{k-k}} + 1)....(a^{2^{k-2}d} + 1)(a^{2^{k-1}d} + 1)$$
$$= (a^d - 1)\prod_{i=0}^{k-1}(a^{2^i d} + 1) \qquad (2)$$

We have $a^d - 1 = a^{3^l m} - 1$.
Base on $(a^3 - b^3) = (a - b)(a^2 + ab + b^2)$ we expand

$$a^{3^l m} - 1$$
$$= (a^{3^{l-1}m} - 1)(a^{2.3^{l-1}m} + a^{3^{l-1}m} + 1)$$
$$= (a^{3^{l-2}m} - 1)(a^{2.3^{l-2}m} + a^{3^{l-2}m} + 1)(a^{2.3^{l-1}m} + a^{3^{l-1}m} + 1)$$
$$= (a^{3^{l-l}m} - 1)(a^{2.3^{l-l}m} + a^{3^{l-l}m} + 1)...(a^{2.3^{l-1}m} + a^{3^{l-1}m} + 1)$$
$$= (a^m - 1)\prod_{j=0}^{l-1}(a^{2.3^j m} + a^{3^j m} + 1) \qquad (3)$$

From (2) and (3), we extend (1) into:

$$a^{2^k 3^l m} - 1 = 0 \ (mod \ n)$$

=> $$(a^m - 1)\prod_{j=0}^{l-1}(a^{2.3^j m} + a^{3^j m} + 1)\prod_{i=0}^{k-1}(a^{2^i d} + 1) = 0 \ (mod \ n) \qquad (4)$$

If (1) is TRUE then one of the factors in (4) must $= 0 \ (mod \ n)$.

From the algorithm:
Part 2: Check if $(a^m - 1) = 0 \ (mod \ n)$
Part 3: Check if $(a^{2.3^j m} + a^{3^j m} + 1) = 0 \ (mod \ n) \ \forall \ j \in [0, l - 1]$
Part 4: Check if $(a^{2^i d} + 1) = 0 \ (mod \ n) \ \forall \ i \in [0, k - 1]$
Therefore, if n is prime then the algorithm will stop at the factor that $= 0 \ (mod \ n)$