(1)

$$\begin{cases} a = q_a m + r_a \\ b = q_b m + r_b \end{cases} \qquad \begin{cases} r_a = a \,\%\, m \\ r_b = b \,\%\, m \end{cases}$$

$$ab \,\%\, m = (q_a m + r_a)(q_b m + r_b) \,\%\, m = (q_a q_b m^2 + q_a r_b m + r_a q_b m + r_a r_b) \,\%\, m$$
$$= \big((q_a q_b m + q_a r_b + r_a q_b)m + r_a r_b\big) \,\%\, m = r_a r_b \,\%\, m = (a \,\%\, m)(b \,\%\, m) \,\%\, m$$

(2)

$$r = b^e \,\%\, m = b^{\sum_{k=0}^{n-1} 2^k e_k} \,\%\, m = b^{2^{n-1} e_{n-1} + \sum_{k=0}^{n-2} 2^k e_k} \,\%\, m$$
$$= b^{2^{n-1} e_{n-1}} b^{\sum_{k=0}^{n-2} 2^k e_k} \,\%\, m = \left(b^{2^{n-1} e_{n-1}} \,\%\, m\right)\left(b^{\sum_{k=0}^{n-2} 2^k e_k} \,\%\, m\right) \,\%\, m$$
$$= \left(b^{2^{n-1}} \,\%\, m\right)\left(b^{\sum_{k=0}^{n-2} 2^k e_k} \,\%\, m\right) \,\%\, m \qquad (e_{n-1} = 1)$$

$$b^{2^{n-1}} \,\%\, m = b^{2^{n-2+1}} \,\%\, m = b^{2^{n-2} 2} \,\%\, m = \left(b^{2^{n-2}}\right)^2 \,\%\, m$$
$$= b^{2^{n-2}} b^{2^{n-2}} \,\%\, m = \left(b^{2^{n-2}} \,\%\, m\right)\left(b^{2^{n-2}} \,\%\, m\right) \,\%\, m = \left(b^{2^{n-2}} \,\%\, m\right)^2 \,\%\, m$$

(3)

$$b^{\sum_{k=0}^{n-1} 2^k e_k} \,\%\, m = \left(b^{2^{n-1}} \,\%\, m\right)\left(b^{\sum_{k=0}^{n-2} 2^k e_k} \,\%\, m\right) \,\%\, m \qquad (e_{n-1} = 1)$$

```
if e_k = 1 then
        r ← br % m
end if
```

$$b^{2^{n-1}} \,\%\, m = \left(b^{2^{n-2}} \,\%\, m\right)^2 \,\%\, m$$

$$\boxed{b \leftarrow b^2 \,\%\, m}$$

(4)

$$b^{2^0 e_0} \% \, m = b^{e_0} \% \, m = b \% \, m \qquad (e_0 = 1)$$

$$br \% \, m = b \% \, m$$

$$\boxed{r \leftarrow 1}$$

(5)

$r \leftarrow 1$

for k from 0 to $(n-1)$ do

    if $e_k = 1$ then

        $r \leftarrow br \% \, m$

    end if

    $b \leftarrow b^2 \% \, m$

end for loop

```
def pow(b, e, m):
   r = 1
   while e != 0:
      if e & 1 == 1:
         r = r * b % m
      b = b * b % m
      e >>= 1
   return r
```