```
> with (LinearAlgebra[Modular]):

> MODBASE := 3;              #The base for the prime-power modulus
  MODPOWER := 3;             #The exponent for the prime-power
  modulus
  MOD := MODBASE^MODPOWER;   #The modulus
  omega := 6;                #The cycle length for A modulo MODBASE^
  (MODPOWER-1)(see below); the program doesn't compute it
  automatically!
```

$$MODBASE := 3$$

$$MODPOWER := 3$$

$$MOD := 27$$

$$\omega := 6 \tag{1}$$

```
> #A is the matrix of interest. "omega" should be the cycle length
  of A modulo MODBASE^(MODPOWER-1)
  #B is the "p^2" digit we're adding to A to create our lift

  A := Matrix([[2, 0, 0],
               [0, 2, 0],
               [0, 0, 2]]);
  B := Matrix([[0, 0, 0],
               [MODBASE^(MODPOWER-1), 0, 0],
               [0, 0, 0]])
```

$$A := \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

$$B := \begin{bmatrix} 0 & 0 & 0 \\ 9 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2}$$

```
> #These next two lines compute A^omega mod MOD and (A+B)^omega mod
  MOD, respectfully
  #The weird part is that both computations are the same despite
  using different lifts of A

  MatrixPower(MOD, A, omega);
  MatrixPower(MOD, A+B, omega)
```

$$\begin{bmatrix} 10 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 10 \end{bmatrix}$$

$$\tag{3}$$

$$\begin{bmatrix} 10 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 10 \end{bmatrix} \quad (3)$$

```
> #However, if we change B to add a "p" digit rather than a "p^2"
  digit, the computations will be different...

  B := Matrix([[0, 0, 0],
               [MODBASE, 0, 0],
               [0, 0, 0]])
```

$$B := \begin{bmatrix} 0 & 0 & 0 \\ 3 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (4)$$

```
> MatrixPower(MOD, A, omega);
  MatrixPower(MOD, A+B, omega)
```

$$\begin{bmatrix} 10 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 10 \end{bmatrix}$$

$$\begin{bmatrix} 10 & 0 & 0 \\ 9 & 10 & 0 \\ 0 & 0 & 10 \end{bmatrix} \quad (5)$$

```
> #No matter what matrix I choose, adding a "p^2" digit mod p^3
  doesn't seem to change the omega-th iteration of the lifted
  matrix, while adding a "p" digit DOES change it.

  #If we were to expand out the expressions we get for the
  different iterations of A+B, we'd get something like:
  #
  #   (A+B)^1 = A   + B                                    mod p^3
  #   (A+B)^2 = A^2 + AB + BA                              mod p^3
  (B^2 = 0 mod p^3)
  #   (A+B)^3 = A^3 + (A^2)B + ABA + B(A^2)                mod p^3
  #   (A+B)^4 = A^4 + (A^3)B + (A^2)BA + AB(A^2) + B(A^3) mod p^3
  #     . . .
  #   (A+B)^n = A^n + sum((A^(k-1-i)).B.(A^i), i=0..n-1)  mod p^3

  (A+B)^n = A^n + sum((A^(n-1-i)).B.(A^i), i=0..n-1);
```

$$\begin{bmatrix} 2 & 0 & 0 \\ 3 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}^n = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}^n + \left(\sum_{i=0}^{n-1} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}^{n-i-1} \cdot \begin{bmatrix} 0 & 0 & 0 \\ 3 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}^i \right) \quad (6)$$

```
> #These next constants are for helping to generate specific terms
  in the summation above

  MAX := omega-1;   #This acts as "n-1" in the above summation
  TERM := 5;  #This acts as  "i"  in the above summation
```

$$MAX := 5$$

$$TERM := 5 \tag{7}$$

```
> #This line computes a specific term in the summation above
  # i.e. it computes (A^(MAX-TERM)).B.(A^TERM) mod MOD

  Multiply(MOD, MatrixPower(MOD, A, MAX-TERM), Multiply(MOD, B,
  MatrixPower(MOD, A, TERM))) mod MOD
```

$$\begin{bmatrix} 0 & 0 & 0 \\ 18 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{8}$$

```
> #This term computes the full summation term from above, using the
  value of MAX as "n-1"

  add(Multiply(MOD, Multiply(MOD, MatrixPower(MOD, A, MAX-i), B),
  MatrixPower(MOD, A, i)), i=0..MAX) mod MOD
```

$$\begin{bmatrix} 0 & 0 & 0 \\ 12 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{9}$$

```
> #If we set B back to a "p^2" digit, the summation evaluates to 0
  when MAX = omega-1:

  B := Matrix([[0, 0, 0],
               [MODBASE^(MODPOWER-1), 0, 0],
               [0, 0, 0]]):
  MAX := omega - 1:
  add(Multiply(MOD, Multiply(MOD, MatrixPower(MOD, A, MAX-i), B),
  MatrixPower(MOD, A, i)), i=0..MAX) mod MOD
```

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{10}$$