

with(LinearAlgebra);

[&x, Add, Adjoint, BackwardSubstitute, BandMatrix, Basis, BezoutMatrix, BidiagonalForm, BilinearForm, CharacteristicMatrix, CharacteristicPolynomial, Column, ColumnDimension, ColumnOperation, ColumnSpace, CompanionMatrix, ConditionNumber, ConstantMatrix, ConstantVector, Copy, CreatePermutation, CrossProduct, DeleteColumn, DeleteRow, Determinant, Diagonal, DiagonalMatrix, Dimension, Dimensions, DotProduct, EigenConditionNumbers, Eigenvalues, Eigenvectors, Equal, ForwardSubstitute, FrobeniusForm, GaussianElimination, GenerateEquations, GenerateMatrix, Generic, GetResultDataType, GetResultShape, GivensRotationMatrix, GramSchmidt, HankelMatrix, HermiteForm, HermitianTranspose, HessenbergForm, HilbertMatrix, HouseholderMatrix, IdentityMatrix, IntersectionBasis, IsDefinite, IsOrthogonal, IsSimilar, IsUnitary, JordanBlockMatrix, JordanForm, KroneckerProduct, LA_Main, LUdecomposition, LeastSquares, LinearSolve, Map, Map2, MatrixAdd, MatrixExponential, MatrixFunction, MatrixInverse, MatrixMatrixMultiply, MatrixNorm, MatrixPower, MatrixScalarMultiply, MatrixVectorMultiply, MinimalPolynomial, Minor, Modular, Multiply, NoUserValue, Norm, Normalize, NullSpace, OuterProductMatrix, Permanent, Pivot, PopovForm, QRdecomposition, RandomMatrix, RandomVector, Rank, RationalCanonicalForm, ReducedRowEchelonForm, Row, RowDimension, RowOperation, RowSpace, ScalarMatrix, ScalarMultiply, ScalarVector, SchurForm, SingularValues, SmithForm, StronglyConnectedBlocks, SubMatrix, SubVector, SumBasis, SylvesterMatrix, ToeplitzMatrix, Trace, Transpose, TridiagonalForm, UnitVector, VandermondeMatrix, VectorAdd, VectorAngle, VectorMatrixMultiply, VectorNorm, VectorScalarMultiply, ZeroMatrix, ZeroVector, Zip]

(1)

```
> lucas := proc(n)
  local M, i, L;
  M := 2^n - 1 : L := 4 :
  for i from 1 to n - 2 do
    L := L^2 - 2 mod M: od;
  evalb(L = 0);
end;
```

lucas := proc(n) (2)

```
  local M, i, L;
```

```
  M := 2^n - 1; L := 4; for i to n - 2 do L := mod(L^2 - 2, M) end do; evalb(L = 0)
```

```
end proc
```

```
> lucas(126);
```

false (3)

```
> isprime(2127 - 1);
```

true (4)

```
> M := RandomMatrix(2, 2);
```

(5)

$$M := \begin{bmatrix} 50 & -16 \\ 10 & -9 \end{bmatrix} \quad (5)$$

> *Power*(*M*, 10);

$$\text{Power} \left(\begin{bmatrix} -32 & -4 \\ -74 & 27 \end{bmatrix}, 10 \right) \quad (6)$$

> ?*Power*

> *puissance* := **proc**(*M*, *n*, *p*)

local *x*, *y*, *m*,

m := *n*;

x := *copy*(*M*);

y := *IdentityMatrix*(2);

while *m* ≠ 0 **do**

if *m* mod 2 = 1 **then** *y* := *x.y* mod *p* **fi**;

x := *x*² mod *p*;

m := floor($\frac{m}{2}$);

od;

y;

end;

> *L* := *Matrix*([[1, 0], [0, 2]]);

$$L := \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \quad (7)$$

> *puissance*(*L*, 5, 7);

$$\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \quad (8)$$

> *IdentityMatrix*(2); *a* := *rand*(1..7); *a*;

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

a := **proc**() **proc**() **option builtin = RandNumberInterface**; **end proc**(6, 7, 3) + 1 **end proc**

a \quad (9)

>

> *M*⁸⁷⁴⁸⁴⁸⁴⁵;

Warning, computation interrupted

> %mod 7;

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad (10)$$

> *puissance*(*M*, 8747784578777584845, 47);

$$\begin{bmatrix} 11 & 2 \\ 34 & 36 \end{bmatrix}$$

(11)

> *lucastest* := **proc**(*N*, *k*, *L*)

local *S*, *D*, *P*, *W*, *i*, *j*, *C*, *n*, *A*, *B*, *v*, *X*, *V*;

i := 0 : *n* := *nops*(*L*) : *W* := *Transpose*(*Matrix*([1, 0])) :

while *i* < *k* **do**:

S := *RandomTools*[*Generate*](*integer*(*range*=1..*N*)) : *P*

:= *RandomTools*[*Generate*](*integer*(*range*=1..*N*)) :

D := *S*² - 4·*P* : *A* := *Matrix*([[*S*, 1], [-*P*, 0]]) : *X* := *puissance*(*A*, *N*, *N*) : *V* := *X*·*W*:

if *igcd*(*N*, *D*·*P*) ≠ 1 **or** *V*[1, 1] **mod** *N* ≠ 0 **then** *i* := *i* + 1 :

else *j* := 1 : **while** *j* ≤ *n* **do** *B* := *puissance*(*A*, $\frac{(N+1)}{L[j]} - 1, N$) : *C* := *B*·*W*:

if *igcd*(*C*[1, 1], *N*) = 1 **then** *j* := *j* + 1 : **else** *j* := *n* + 15 : **fi**:**od**:

if *j* = *n* + 1 **then** **return**(*premier*);

else *i* := *i* + 1 : **fi**:

fi:

od:

if *i* = *k* **then** **return**(*pas premier*);

fi:

end:

> *L* := [2, 3, 7, 5, 47] : *isprime*((3·7·27·25·47·81·16) - 1);

false

(12)

> *debug*(*lucastest*); *lucastest*((3·7·27·25·47·81·16) - 1, 4, *L*);

lucastest

{--> *enter lucastest*, *args* = 863427599, 4, [2, 3, 7, 5, 47]

i := 0

n := 5

$$W := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

S := 102723287

P := 316773881

D := 10552072424988845

$$A := \begin{bmatrix} 102723287 & 1 \\ -316773881 & 0 \end{bmatrix}$$

$$X := \begin{bmatrix} 120879045 & 781481943 \\ 728907116 & 639254715 \end{bmatrix}$$

$$V := \begin{bmatrix} 120879045 \\ 728907116 \end{bmatrix}$$

$$i := 1$$

$$S := 388203733$$

$$P := 544418953$$

$$D := 150702136137459477$$

$$A := \begin{bmatrix} 388203733 & 1 \\ -544418953 & 0 \end{bmatrix}$$

$$X := \begin{bmatrix} 351196014 & 783481289 \\ 264156957 & 269067724 \end{bmatrix}$$

$$V := \begin{bmatrix} 351196014 \\ 264156957 \end{bmatrix}$$

$$i := 2$$

$$S := 366222185$$

$$P := 249861828$$

$$D := 134118687786726913$$

$$A := \begin{bmatrix} 366222185 & 1 \\ -249861828 & 0 \end{bmatrix}$$

$$X := \begin{bmatrix} 189690468 & 418613806 \\ 778814241 & 334473618 \end{bmatrix}$$

$$V := \begin{bmatrix} 189690468 \\ 778814241 \end{bmatrix}$$

$$i := 3$$

$$S := 76338301$$

$$P := 5441983$$

$$D := 5827536177798669$$

$$A := \begin{bmatrix} 76338301 & 1 \\ -5441983 & 0 \end{bmatrix}$$

$$X := \begin{bmatrix} 165311200 & 7023668 \\ 394526487 & 7540548 \end{bmatrix}$$

$$V := \begin{bmatrix} 165311200 \\ 394526487 \end{bmatrix}$$

$$i := 4$$

```

<-- exit lucastest (now at top level) = `*(pas, `*(premier))}
      pas premier
> L := [2, 3, 17]: lucastest(101, 5, L);
{--> enter lucastest, args = 101, 5, [2, 3, 17]
      i:= 0
      n:= 3
      W:=  $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ 
      S:= 100
      P:= 70
      D:= 9720
      A:=  $\begin{bmatrix} 100 & 1 \\ -70 & 0 \end{bmatrix}$ 
      X:=  $\begin{bmatrix} 100 & 1 \\ 31 & 0 \end{bmatrix}$ 
      V:=  $\begin{bmatrix} 100 \\ 31 \end{bmatrix}$ 
      i:= 1
      S:= 36
      P:= 36
      D:= 1152
      A:=  $\begin{bmatrix} 36 & 1 \\ -36 & 0 \end{bmatrix}$ 
      X:=  $\begin{bmatrix} 0 & 100 \\ 36 & 36 \end{bmatrix}$ 
      V:=  $\begin{bmatrix} 0 \\ 36 \end{bmatrix}$ 
      j:= 1
      B:=  $\begin{bmatrix} 0 & 17 \\ 95 & 95 \end{bmatrix}$ 
      C:=  $\begin{bmatrix} 0 \\ 95 \end{bmatrix}$ 
      j:= 18
      i:= 2
      S:= 10

```

$P := 40$

$D := -60$

$$A := \begin{bmatrix} 10 & 1 \\ -40 & 0 \end{bmatrix}$$

$$X := \begin{bmatrix} 0 & 100 \\ 40 & 10 \end{bmatrix}$$

$$V := \begin{bmatrix} 0 \\ 40 \end{bmatrix}$$

$j := 1$

$$B := \begin{bmatrix} 43 & 18 \\ 88 & 65 \end{bmatrix}$$

$$C := \begin{bmatrix} 43 \\ 88 \end{bmatrix}$$

$j := 2$

$$B := \begin{bmatrix} 19 & 82 \\ 53 & 7 \end{bmatrix}$$

$$C := \begin{bmatrix} 19 \\ 53 \end{bmatrix}$$

$j := 3$

$$B := \begin{bmatrix} 19 & 4 \\ 42 & 80 \end{bmatrix}$$

$$C := \begin{bmatrix} 19 \\ 42 \end{bmatrix}$$

$j := 4$

```
<-- exit lucastest (now at top level) = premier}
      premier
```

```
>
```

(14)