Assignment 2 Question 3(a) Padic Linear Solver

```
> PadicSolve := proc(A::Matrix,b::Vector,p::integer) local n,Ai,ek,u,
  k,xk,x;
  uses LinearAlgebra;
    n := RowDimension(A);
    Ai := Inverse(A) mod p;
    ek := b;
    u := Vector(n); # u = 0
    for k from 0 to 1000 do
      xk := Ai.ek mod p;
      u := u + p^k*xk;
      x := iratrecon(u,p^(k+1));
      if x<>FAIL and Equal(b-A.x,Vector(n)) then
         printf("%d lifting steps\n",k+1); break
      fi;
      ek := (ek-A.xk)/p;
    od;
    x;
  end:
```

```
> A := Matrix([[23,41],[11,18]]);
  b := <4,21>;
  x := PadicSolve(A,b,19);
  A.x-b;
```

$$A := \begin{bmatrix} 23 & 41 \\ 11 & 18 \end{bmatrix}$$

$$b := \begin{bmatrix} 4 \\ 21 \end{bmatrix}$$

```
5 lifting steps
```

$$x := \begin{bmatrix} \frac{789}{37} \\ -\frac{439}{37} \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \textbf{(1)}$$

```
> with(LinearAlgebra):
  B := 2^16;
  m := 3;
  U := rand(B^m):
  n := 50;
```

```
A := RandomMatrix(n,n,generator=U):
b := RandomVector(n,generator=U):
p := 2^31-1;
x := PadicSolve(A,b,p):
convert(A.x-b,set);
```

$$B := 65536$$

$$m := 3$$

$$n := 50$$

$$p := 2147483647$$

157 lifting steps

$$\{0\} \quad \textbf{(2)}$$

```
> y := [1,0,-1/2,2/3,4,3/4,-2,-3,0,-1];
  y := map(op,[y$5]);
  x := Vector(y):
  b := A.x:
  # We must clear the fractions from Ax=b
  L := ilcm(seq(denom(b[i]),i=1..n));
  A := L*A:
  b := L*b:
  x := PadicSolve(A,b,p):
  convert(A.x-b,set);
```

$$y := \left[1, 0, -\frac{1}{2}, \frac{2}{3}, 4, \frac{3}{4}, -2, -3, 0, -1\right]$$

$$y := \left[1, 0, -\frac{1}{2}, \frac{2}{3}, 4, \frac{3}{4}, -2, -3, 0, -1, 1, 0, -\frac{1}{2}, \frac{2}{3}, 4, \frac{3}{4}, -2, -3, 0, -1, 1, 0, -\frac{1}{2}, \frac{2}{3}, 4, \frac{3}{4}, -2, -3, 0, -1, 1, 0, -\frac{1}{2}, \frac{2}{3}, 4, \frac{3}{4}, -2, -3, 0, -1, 1, 0, -\frac{1}{2}, \frac{2}{3}, 4, \frac{3}{4}, -2, -3, 0, -1\right]$$

$$L := 1$$

1 lifting steps

$$\{0\} \quad \textbf{(3)}$$