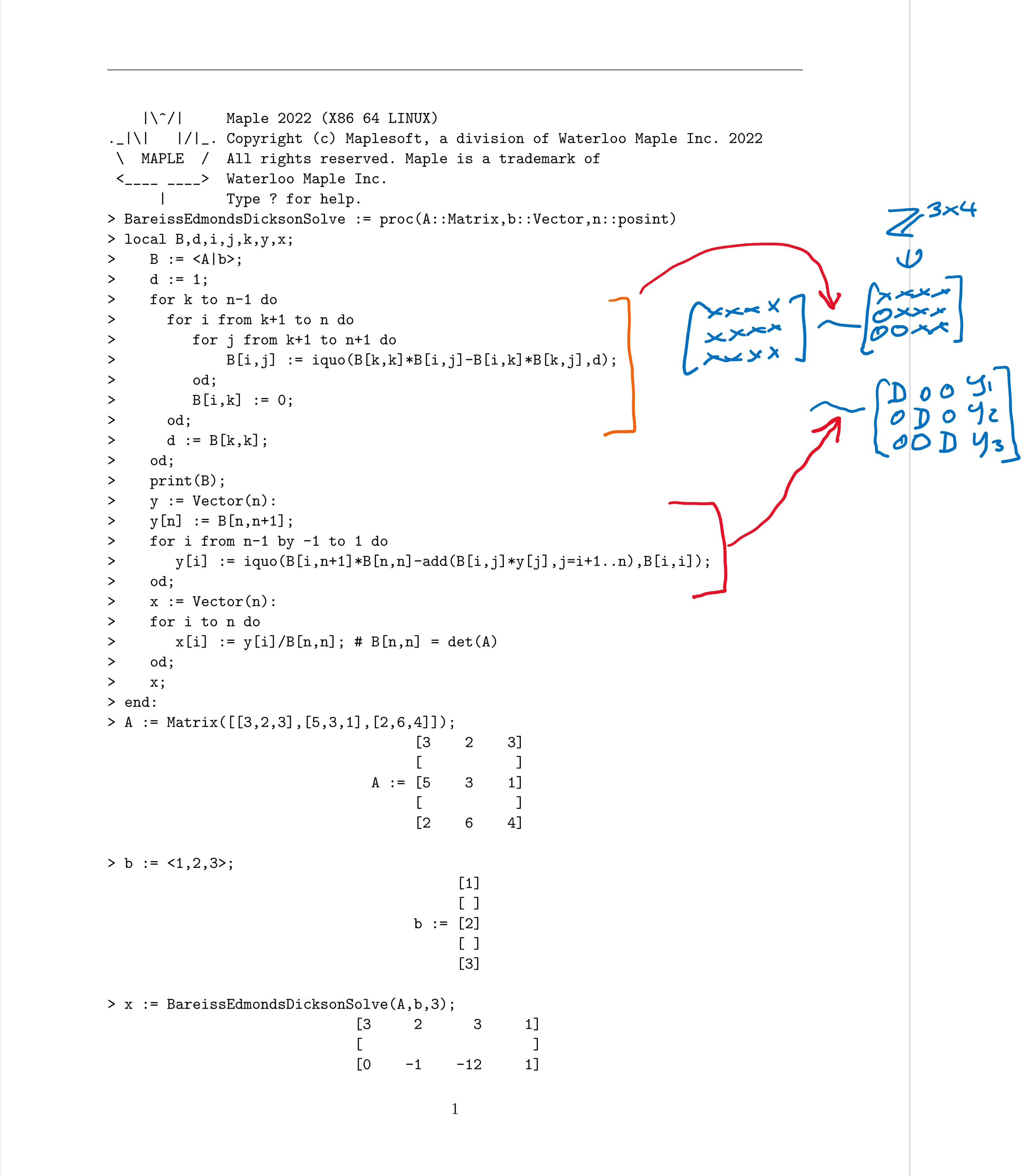
Handouts

September 28, 2023 8:44 AM



```
    |\^/|     Maple 2022 (X86 64 LINUX)
._|\|   |/|_. Copyright (c) Maplesoft, a division of Waterloo Maple Inc. 2022
 \  MAPLE  /  All rights reserved. Maple is a trademark of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> BareissEdmondsDicksonSolve := proc(A::Matrix,b::Vector,n::posint)
> local B,d,i,j,k,y,x;
>    B := <A|b>;
>    d := 1;
>    for k to n-1 do
>      for i from k+1 to n do
>         for j from k+1 to n+1 do
>             B[i,j] := iquo(B[k,k]*B[i,j]-B[i,k]*B[k,j],d);
>         od;
>         B[i,k] := 0;
>      od;
>      d := B[k,k];
>    od;
>    print(B);
>    y := Vector(n):
>    y[n] := B[n,n+1];
>    for i from n-1 by -1 to 1 do
>       y[i] := iquo(B[i,n+1]*B[n,n]-add(B[i,j]*y[j],j=i+1..n),B[i,i]);
>    od;
>    x := Vector(n):
>    for i to n do
>       x[i] := y[i]/B[n,n]; # B[n,n] = det(A)
>    od;
>    x;
> end:
> A := Matrix([[3,2,3],[5,3,1],[2,6,4]]);
                                    [3    2    3]
                                    [           ]
                               A := [5    3    1]
                                    [           ]
                                    [2    6    4]

> b := <1,2,3>;
                                         [1]
                                         [ ]
                                    b := [2]
                                         [ ]
                                         [3]

> x := BareissEdmondsDicksonSolve(A,b,3);
                             [3     2      3     1]
                             [                    ]
                             [0    -1    -12     1]
```

$\mathbb{Z}^{3\times 4}$

$\Downarrow$

$$\begin{bmatrix} x&x&x&x\\ x&x&x&x\\ x&x&x&x\end{bmatrix} \sim \begin{bmatrix} x&x&x&x\\ 0&x&x&x\\ 0&0&x&x\end{bmatrix} \sim \begin{bmatrix} D&0&0&y_1\\ 0&D&0&y_2\\ 0&0&D&y_3\end{bmatrix}$$

```
                              [                    ]
                              [0     0     54    -7]

                                        [5/54]
                                        [    ]
                                        [5/9 ]
                                   x := [    ]
                                        [ -7 ]
                                        [ -- ]
                                        [ 54 ]

> A.x = b;
                                    [1]   [1]
                                    [ ]   [ ]
                                    [2] = [2]
                                    [ ]   [ ]
                                    [3]   [3]
```

```
> restart;
  with(LinearAlgebra):
> A,b  := RandomMatrix(3,3), RandomVector(3);
```

$$A,\, b := \begin{bmatrix} 27 & 99 & 92 \\ 8 & 29 & -31 \\ 69 & 44 & 67 \end{bmatrix}, \begin{bmatrix} -32 \\ -74 \\ -4 \end{bmatrix} \tag{1}$$

```
> x := LinearSolve(A,b);
```

$$x := \begin{bmatrix} -\frac{54207}{163622} \\ -\frac{207597}{163622} \\ \frac{182389}{163622} \end{bmatrix} \tag{2}$$

```
> p := prevprime(10^4);
```

$$p := 9973 \tag{3}$$

Solve $A \cdot x = b$ modulo p, p^2, p^3, ...

```
> u := x mod p;
```

$$u := \begin{bmatrix} 4427 \\ 6677 \\ 1922 \end{bmatrix} = x_0 \tag{4}$$

```
> y := iratrecon(u,p);
```

$$y := FAIL \tag{5}$$

```
> u := x mod p^2;
```

$$u := \begin{bmatrix} 60351050 \\ 78613863 \\ 95533289 \end{bmatrix} \quad x_0 + x_1 \cdot p \tag{6}$$

```
> y := iratrecon(u,p^2);
```

$$y := FAIL \tag{7}$$

```
> u := x mod p^3;
```

$$u := \begin{bmatrix} 432416140013 \\ 251614797504 \\ 410967804788 \end{bmatrix} = x_0 + x_1 p + x_2 p^2 \tag{8}$$

```
> y := iratrecon(u,p^3);
```

$$y := \begin{bmatrix} -\frac{54207}{163622} \\ -\frac{207597}{163622} \\ \frac{182389}{163622} \end{bmatrix} \tag{9}$$

```
> A.y-b;
```

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

```
> d := ilcm( denom(y[1]), denom(y[2]), denom(y[3]) );
```

$$d := 163622 \tag{11}$$

```
> A.(d*y)-(d*b);
```

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

Check using $\mathbb{Z}$ arithmetic.

```
> ?iratrecon
```

```
    |\^/|     Maple 2022 (X86 64 LINUX)
._|\|   |/|_. Copyright (c) Maplesoft, a division of Waterloo Maple Inc. 2022
 \  MAPLE  /  All rights reserved. Maple is a trademark of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.

> EEA := proc(m,u) local s,t,r,q,i;
>   r[0],r[1] := m,u;
>   # s[0],s[1] := 1,0;
>   t[0],t[1] := 0,1;
>   printf("\n");
>   printf("%4s %10s %10s %10s %12s\n","i","r[i]","t[i]","q[i+1]","r[i]/t[i]");
>   for i from 1 while r[i]<>0 do
>     q[i+1] := iquo(r[i-1],r[i]);
>     r[i+1] := r[i-1]-q[i+1]*r[i];
>     # s[i+1] := s[i-1]-q[i+1]*s[i];
>     t[i+1] := t[i-1]-q[i+1]*t[i];
>     printf("%4d %10d %10d %10d %12a\n",i,r[i],t[i],q[i+1],r[i]/t[i]);
>   od:
> end:

> m := 10^6-17;
                                  m := 999983

> u := 72/109 mod m;
                                  u := 137613
```

$m > 2ND$

$N = D = \lfloor \sqrt{\frac{m}{2}} \rfloor = 700.$

$|n| \leq 700$

$d \leq 700$

```
> EEA(m,u);

   i       r[i]       t[i]     q[i+1]    r[i]/t[i]
   1     137613          1          7       137613
   2      36692         -7          3    -36692/7
   3      27537         22          1     27537/22
   4       9155        -29          3    -9155/29
   5         72        109        127       72/109
   6         11     -13872          6   -11/13872
   7          6      83341          1     6/83341
   8          5     -97213          1    -5/97213
   9          1     180554          5   1/180554
```

```
> u := rand(m)();

                                u := 113500

> EEA(m,u);

   i      r[i]        t[i]     q[i+1]     r[i]/t[i]
   1    113500           1          8        113500
   2     91983          -8          1      -91983/8
   3     21517           9          4       21517/9
   4      5915         -44          3     -5915/44
   5      3772         141          1     3772/141
   6      2143        -185          1    -2143/185
   7      1629         326          1     1629/326
   8       514        -511          3     -514/511
   9        87        1859          5      87/1859
  10        79       -9806          1     -79/9806
  11         8       11665          9     8/11665
  12         7     -114791          1    -7/114791
  13         1      126456          7     1/126456
```