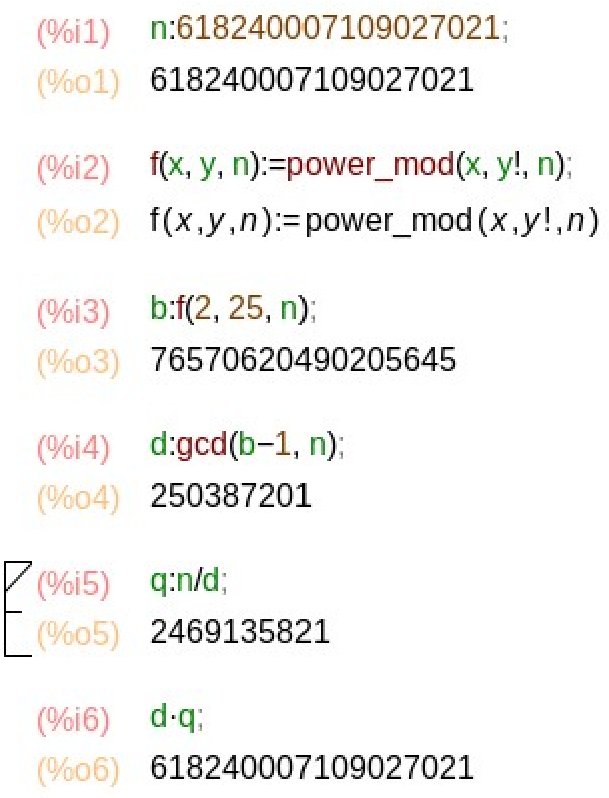
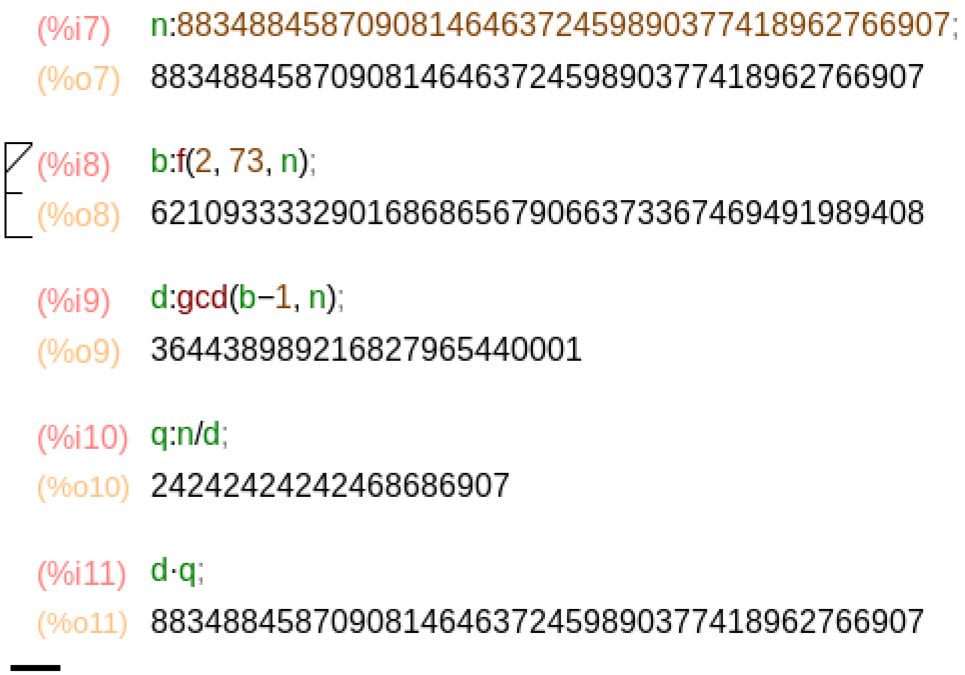
Cole Barbes – Homework #9

#4



```
(%i1)  n:618240007109027021;
(%o1)  618240007109027021

(%i2)  f(x, y, n):=power_mod(x, y!, n);
(%o2)  f(x,y,n):=power_mod(x,y!,n)

(%i3)  b:f(2, 25, n);
(%o3)  76570620490205645

(%i4)  d:gcd(b−1, n);
(%o4)  250387201

(%i5)  q:n/d;
(%o5)  2469135821

(%i6)  d·q;
(%o6)  618240007109027021
```

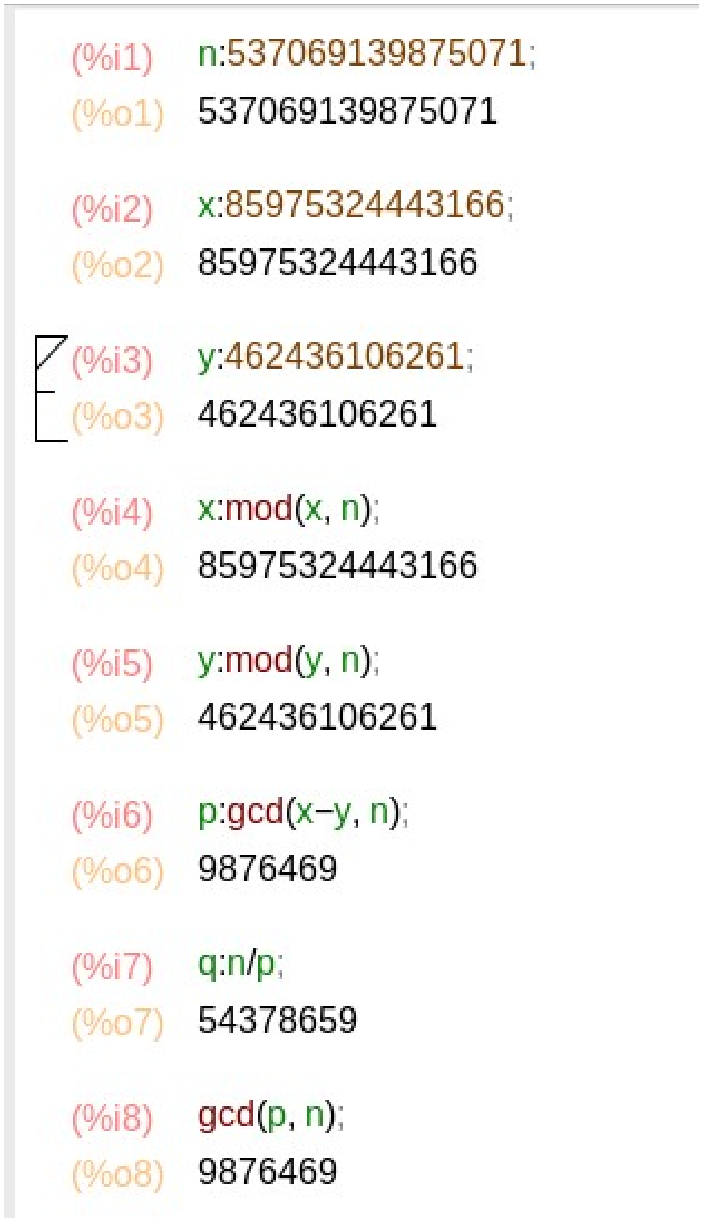
#5



```
(%i7)  n:883488458709081464637245989037741896276690 7;
```

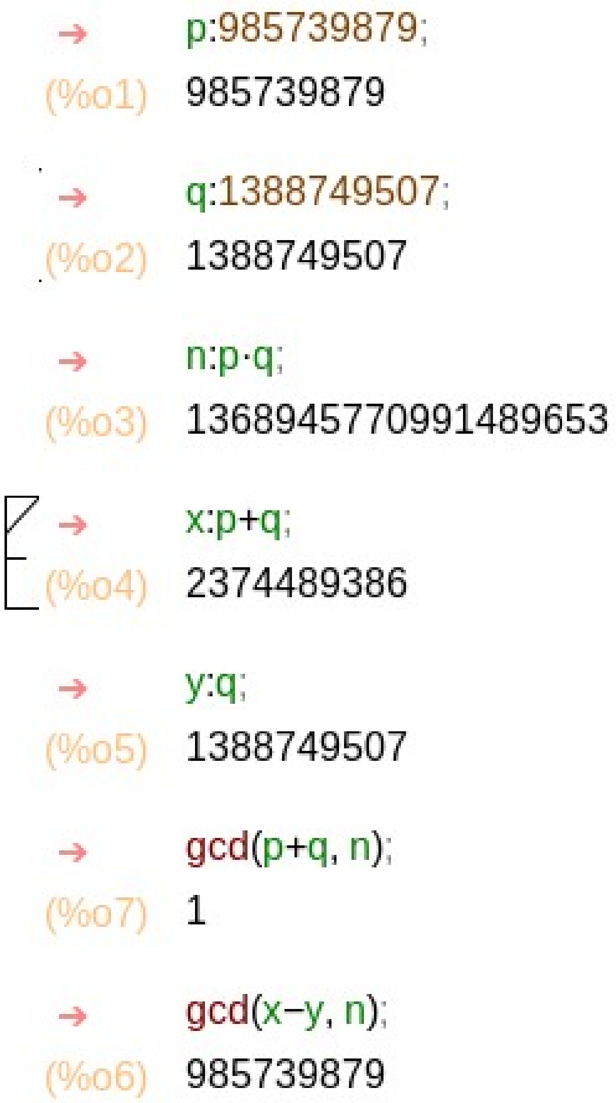
```
(%i7)  n:8834884587090814646372459890377418962766907;
(%o7)  8834884587090814646372459890377418962766907

(%i8)  b:f(2, 73, n);
(%o8)  6210933332901686865679066373367469491989408

(%i9)  d:gcd(b−1, n);
(%o9)  3644389892168279654400001

(%i10) q:n/d;
(%o10) 242424242424268686907

(%i11) d·q;
(%o11) 8834884587090814646372459890377418962766907
```

#6



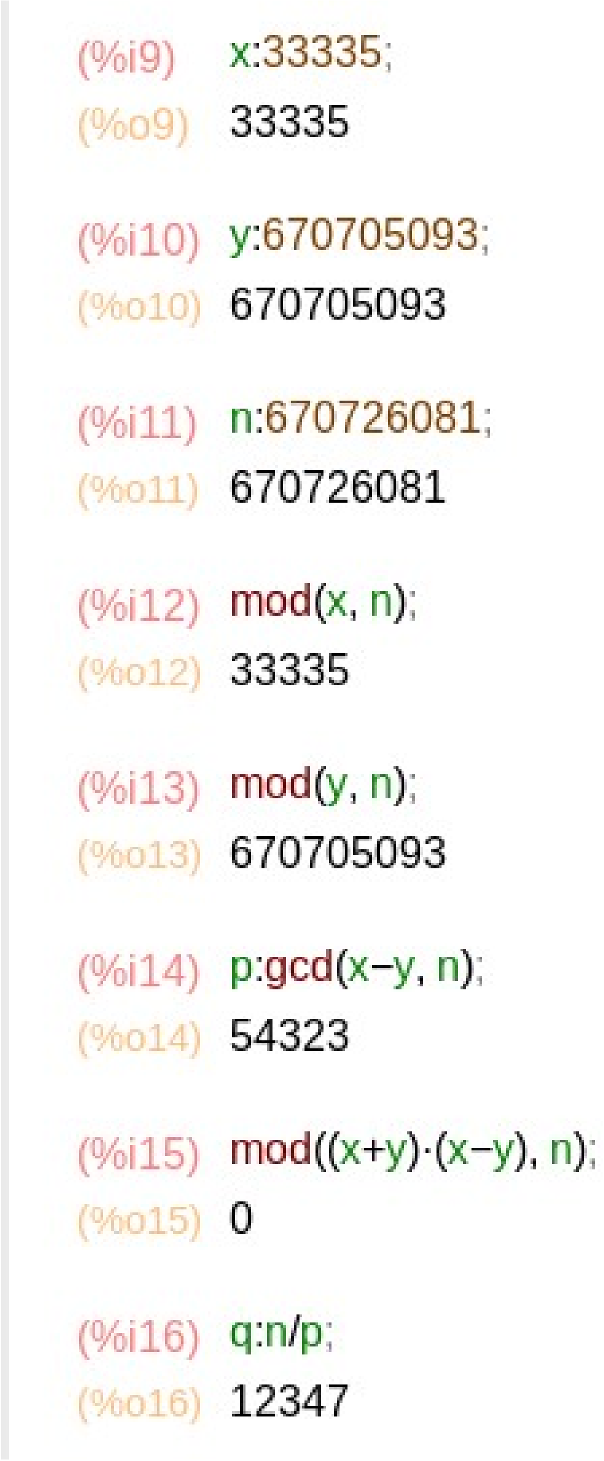
```
(%i1) n:537069139875071;
(%o1) 537069139875071

(%i2) x:85975324443166;
(%o2) 85975324443166

(%i3) y:462436106261;
(%o3) 462436106261

(%i4) x:mod(x, n);
(%o4) 85975324443166

(%i5) y:mod(y, n);
(%o5) 462436106261

(%i6) p:gcd(x−y, n);
(%o6) 9876469

(%i7) q:n/p;
(%o7) 54378659

(%i8) gcd(p, n);
(%o8) 9876469
```

#7

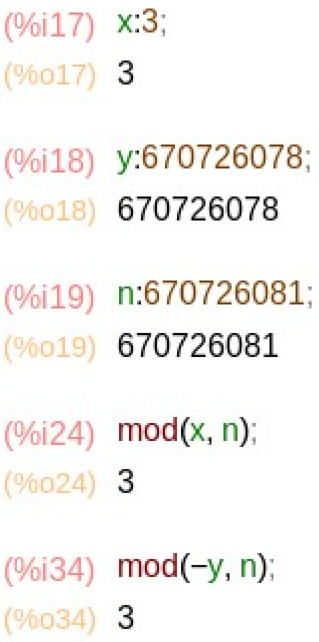


```
→       p:985739879;
(%o1)   985739879

→       q:1388749507;
(%o2)   1388749507

→       n:p·q;
(%o3)   1368945770991489653

→       x:p+q;
(%o4)   2374489386

→       y:q;
(%o5)   1388749507

→       gcd(p+q, n);
(%o7)   1

→       gcd(x−y, n);
(%o6)   985739879
```

#8: the information in part 2 is not helpful in factoring n since the x is congruent to -y (mod n)

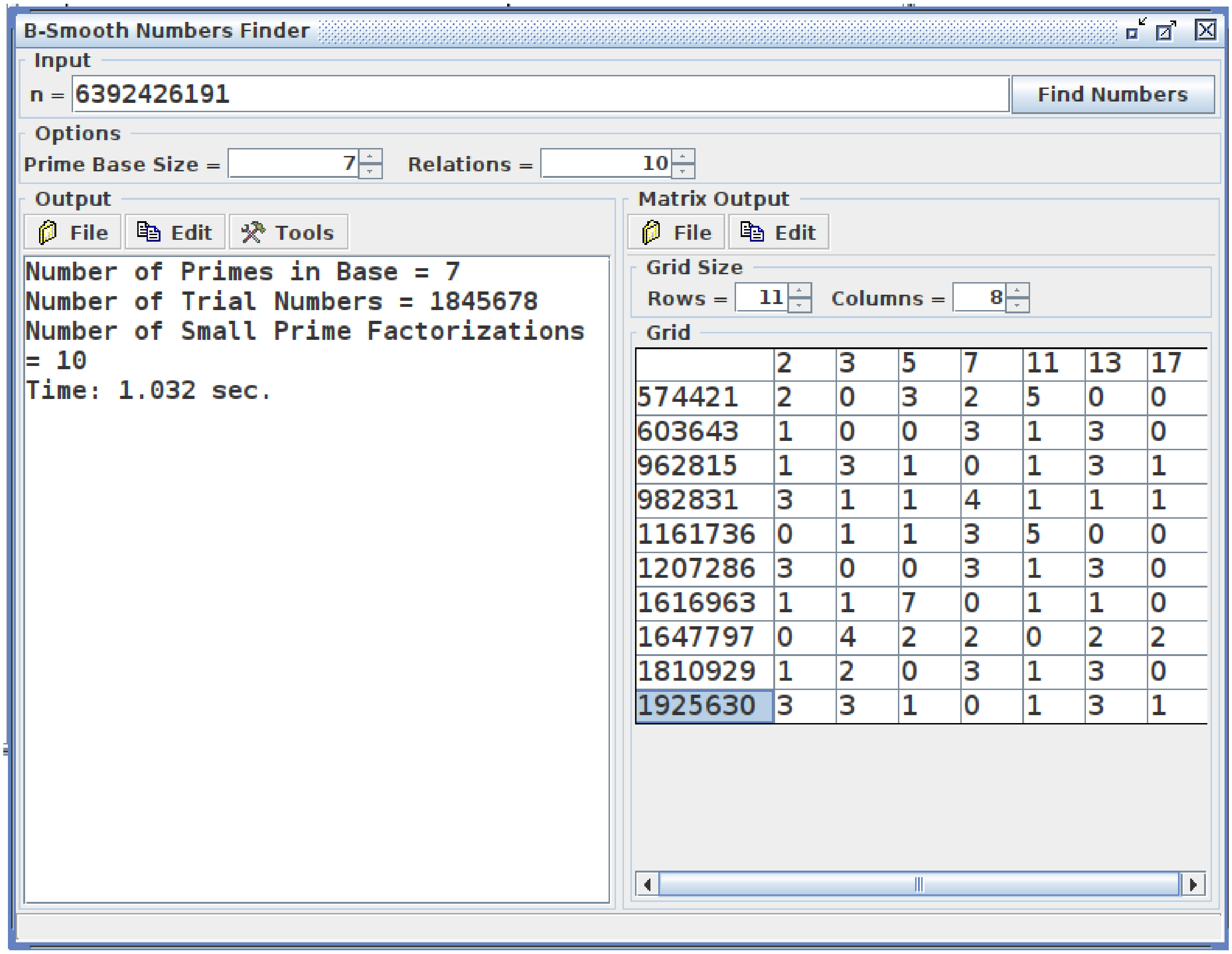


```
(%i9)  x:33335;
(%o9)  33335

(%i10) y:670705093;
(%o10) 670705093

(%i11) n:670726081;
(%o11) 670726081

(%i12) mod(x, n);
(%o12) 33335

(%i13) mod(y, n);
(%o13) 670705093

(%i14) p:gcd(x−y, n);
(%o14) 54323

(%i15) mod((x+y)·(x−y), n);
(%o15) 0

(%i16) q:n/p;
(%o16) 12347
```



```
(%i17) x:3;
(%o17) 3

(%i18) y:670726078;
(%o18) 670726078

(%i19) n:670726081;
(%o19) 670726081

(%i24) mod(x, n);
(%o24) 3

(%i34) mod(−y, n);
(%o34) 3
```

quadratic sieve:
factor n = 6392426191



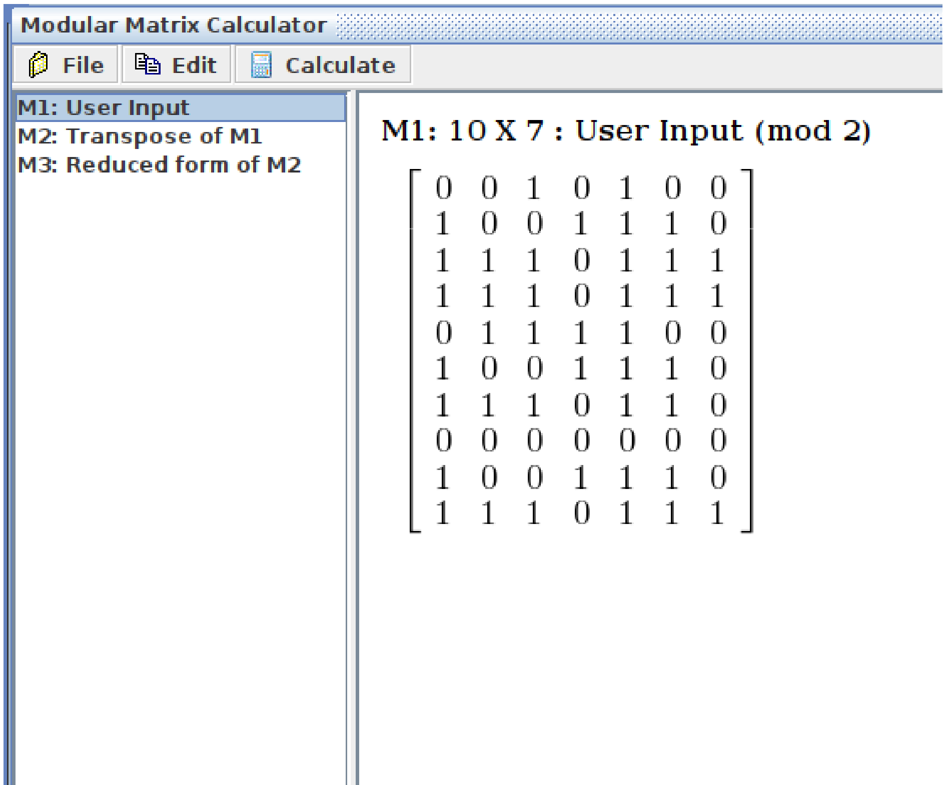
n = 6392426191

Prime Base Size = 7   Relations = 10

```
Number of Primes in Base = 7
Number of Trial Numbers = 1845678
Number of Small Prime Factorizations
= 10
Time: 1.032 sec.
```

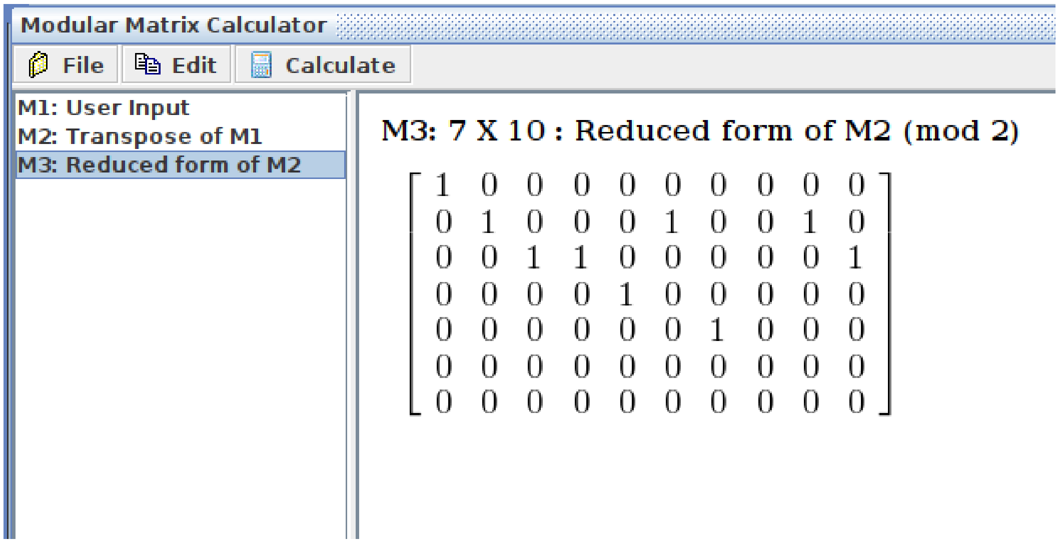
Rows = 11   Columns = 8

	2	3	5	7	11	13	17
574421	2	0	3	2	5	0	0
603643	1	0	0	3	1	3	0
962815	1	3	1	0	1	3	1
982831	3	1	1	4	1	1	1
1161736	0	1	1	3	5	0	0
1207286	3	0	0	3	1	3	0
1616963	1	1	7	0	1	1	0
1647797	0	4	2	2	0	2	2
1810929	1	2	0	3	1	3	0
1925630	3	3	1	0	1	3	1



M1: 10 X 7 : User Input (mod 2)

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



M3: 7 X 10 : Reduced form of M2 (mod 2)

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