Modern Cryptography Spring 2024
Exercises

Xiaoqi LIU
liu09335@gtiit.edu.cn

06/09/2024

Problem Nr.1 *What is the probability that the text "apple'' occurs, when the plaintext source generates independent, identically distributed 1-grams, as described in Example 1.1. Answer the same question when the Markov model of Example 1.3 is used? (01.01)*

Solution.

1) For 1-grams, $Pr_{plain}(apple) = p(a) * p(p) * p(p) * p(l) * p(e) =$

$$= 0.0804 * 0.02 * 0.02 * 0.0414 * 0.1251 = 1.665611424 \times 10^{\wedge} - 7$$

a	0.0804	h	0.0549	o	0.0760	v	0.0099
b	0.0154	i	0.0726	p	0.0200	w	0.0192
c	0.0306	j	0.0016	q	0.0011	x	0.0019
d	0.0399	k	0.0067	r	0.0612	y	0.0173
e	0.1251	l	0.0414	s	0.0654	z	0.0009
f	0.0230	m	0.0253	t	0.0925		
g	0.0196	n	0.0709	u	0.0271		

Probability distributions of 1-grams in English.

2) For Markov model, $Pr_{plain}(apple) = p(a) * p(p|a) * p(p|p) * p(l|p) * p(e|l) =$

$$= 0.0723 * 0.0222 * 0.0581 * 0.0812 * 0.1918 = 1.45235249860176 \times 10^{\wedge} - 6$$

```
ed["a"] = 0.0723; ed["j"] = 0.0006; ed["s"] = 0.0715;
ed["b"] = 0.0060; ed["k"] = 0.0064; ed["t"] = 0.0773;
ed["c"] = 0.0282; ed["l"] = 0.0396; ed["u"] = 0.0272;
ed["d"] = 0.0483; ed["m"] = 0.0236; ed["v"] = 0.0117;
ed["e"] = 0.1566; ed["n"] = 0.0814; ed["w"] = 0.0078;
ed["f"] = 0.0167; ed["o"] = 0.0716; ed["x"] = 0.0030;
ed["g"] = 0.0216; ed["p"] = 0.0161; ed["y"] = 0.0168;
ed["h"] = 0.0402; ed["q"] = 0.0007; ed["z"] = 0.0010;
ed["i"] = 0.0787; ed["r"] = 0.0751;
```

	a	b	c	d	e	f	g	h	i	j	k	l	m
a	0.0011	0.0193	0.0388	0.0469	0.002	0.01	0.0233	0.002	0.048	0.002	0.0103	0.1052	0.0281
b	0.0931	0.0057	0.0016	0.0008	0.3219	0	0	0	0.0605	0.0057	0	0.1242	0.0049
c	0.1202	0	0.0196	0.0004	0.1707	0	0	0.1277	0.0761	0	0.0324	0.0369	0.0015
d	0.1044	0.002	0.0026	0.0218	0.3778	0.0007	0.0132	0.0007	0.1803	0.0033	0	0.0125	0.0178
e	0.066	0.0036	0.0433	0.1194	0.0438	0.0142	0.0125	0.0021	0.0158	0.0005	0.0036	0.0456	0.034
f	0.0838	0	0	0	0.1283	0.0924	0	0	0.1608	0	0	0.0299	0.0009
g	0.1078	0	0	0.0018	0.2394	0	0.0177	0.1281	0.0839	0	0	0.0203	0.0027
h	0.1769	0.0005	0.0014	0.0008	0.5623	0	0	0.0005	0.1167	0	0	0.0016	0.0016
i	0.038	0.0082	0.0767	0.0459	0.0437	0.0129	0.028	0.0002	0.0016	0	0.005	0.0567	0.0297
j	0.1259	0	0	0	0.1818	0	0	0	0.035	0	0	0	0
k	0.0395	0.0028	0	0.0028	0.5282	0.0028	0	0.0198	0.1582	0	0.0113	0.0198	0.0028
l	0.1342	0.0019	0.0022	0.0736	0.1918	0.0105	0.0108	0	0.1521	0	0.0079	0.1413	0.0082
m	0.1822	0.0337	0.0026	0	0.2975	0.001	0	0	0.1345	0	0	0.001	0.0654
n	0.055	0.0004	0.0621	0.1681	0.1212	0.0102	0.1391	0.0013	0.0665	0.0009	0.0066	0.0073	0.0104
o	0.0085	0.0101	0.0162	0.0231	0.0037	0.1299	0.0082	0.0025	0.0092	0.0014	0.0078	0.0416	0.0706
p	0.1359	0	0.0006	0	0.1747	0	0	0.0237	0.0423	0	0	0.0812	0.0073
q	0	0	0	0	0	0	0	0	0	0	0	0	0
r	0.1026	0.0033	0.0172	0.0282	0.2795	0.0031	0.0175	0.0017	0.1181	0	0.0205	0.0164	0.0303
s	0.0604	0.0012	0.0284	0.0027	0.1795	0.0024	0	0.0561	0.1177	0	0.0091	0.0145	0.0112
t	0.0619	0.0003	0.0036	0.0002	0.1417	0.0007	0.0002	0.3512	0.1406	0	0	0.0101	0.0044
u	0.0344	0.0415	0.0491	0.0243	0.0434	0.0052	0.0382	0.001	0.0258	0	0.0014	0.1097	0.0329
v	0.0749	0	0	0.0023	0.6014	0	0	0	0.2569	0	0	0	0.0012
w	0.2291	0.0008	0	0.0032	0.1942	0	0	0.1422	0.2104	0	0	0.0041	0
x	0.0672	0	0.1119	0	0.1269	0	0	0.0075	0.1119	0	0	0	0.0075
y	0.0586	0.0034	0.0103	0.0069	0.2897	0	0	0	0.069	0	0.0034	0.0172	0.0379
z	0.2278	0	0	0	0.4557	0	0	0	0.2152	0	0	0.0127	0

	n	o	p	q	r	s	t	u	v	w	x	y	z
a	0.1878	0.0008	0.0222	0	0.118	0.1001	0.1574	0.0137	0.0212	0.0057	0.0026	0.0312	0.0023
b	0	0.0964	0	0	0.0662	0.0229	0.0049	0.0727	0.0016	0	0	0.1168	0
c	0.0011	0.2283	0	0.0004	0.0426	0.0087	0.0893	0.0347	0	0	0	0.0094	0
d	0.0053	0.0733	0	0.0007	0.0324	0.0495	0.0013	0.0601	0.0099	0.004	0	0.0264	0
e	0.1381	0.004	0.0192	0.0034	0.1927	0.1231	0.0404	0.0048	0.0215	0.0205	0.0152	0.0121	0.0004
f	0.0009	0.2789	0	0	0.1215	0.0026	0.0496	0.0462	0	0	0	0.0043	0
g	0.0451	0.114	0	0	0.1325	0.0256	0.0247	0.0512	0	0	0	0.0053	0
h	0.0038	0.0786	0	0	0.0153	0.0027	0.0233	0.0085	0	0.0011	0	0.0041	0
i	0.2498	0.0893	0.01	0.0008	0.0342	0.1194	0.1135	0.0011	0.025	0	0.0023	0.0002	0.0079
j	0	0.3147	0	0	0.007	0	0	0.3357	0	0	0	0	0
k	0.0565	0.0198	0	0	0.0085	0.1102	0.0028	0.0028	0	0	0	0.0113	0
l	0.0004	0.0778	0.0041	0	0.0034	0.0389	0.0254	0.0269	0.0056	0.0011	0	0.0819	0
m	0.0042	0.1246	0.0722	0	0.0026	0.0244	0.0005	0.0337	0.0005	0	0	0.0192	0
n	0.0194	0.0528	0.0004	0.0007	0.0011	0.0751	0.1641	0.0124	0.0068	0.0018	0.0002	0.0157	0.0004
o	0.219	0.0222	0.0292	0	0.153	0.0357	0.0396	0.0947	0.0334	0.0345	0.0012	0.0041	0.0004
p	0.0006	0.1511	0.0581	0	0.2306	0.018	0.0287	0.0457	0	0	0	0.0017	0
q	0	0	0	0	0	0	0	1	0	0	0	0	0
r	0.0325	0.1114	0.0055	0	0.0212	0.0655	0.0596	0.0192	0.0142	0.0017	0.0002	0.0306	0
s	0.0021	0.0706	0.0386	0.0009	0.0027	0.0836	0.2483	0.0579	0	0.0039	0	0.0081	0
t	0.0015	0.1229	0.0003	0	0.0479	0.0418	0.0213	0.0195	0.0005	0.0088	0	0.0203	0.0005
u	0.1517	0.0019	0.0386	0	0.146	0.1221	0.1255	0.0029	0.0014	0	0.001	0.0014	0.0005
v	0	0.053	0	0	0	0.0023	0	0.0012	0.0012	0	0	0.0058	0
w	0.0357	0.1292	0	0	0.0106	0.0366	0.0016	0	0	0	0	0.0024	0
x	0	0.0075	0.3507	0	0	0	0.1716	0	0	0	0.0373	0	0
y	0.0172	0.2207	0.031	0	0.031	0.1517	0.0172	0.0138	0	0.0103	0	0.0069	0.0034
z	0	0.0506	0	0	0	0	0	0.0127	0	0	0	0	0.0253

3) Use Mathematica to verify my answer:

sourcetext = "apple";

$$\texttt{ed[StringTake[sourcetext, \{1\}]]} * \prod_{i=1}^{\texttt{StringLength[sourcetext]-1}} \texttt{TrPr[[ToCharacterCode[StringTake[sourcetext, \{i\}]] - 96, ToCharacterCode[StringTake[sourcetext, \{i + 1\}]] - 96]]}$$

$\{\{1.45235 \times 10^{-6}\}\}$

Problem Nr.2 *Encrypt the following plaintext using the Vigenère system with the key ''vigenere'': "who is afraid of virginia woolf". (02.03)*

Solution.

First we convert alphabet to corresponding integers, then mod 26: $(m_i + k_i)\ mod\ 26$

Plaintext	w	h	o	i	s	a	f	r	a	i	d	o	f	v	i	r	g	i	n	i	a	w	o	o	l	f
m_i	22	7	14	8	18	0	5	17	0	8	3	14	5	21	8	17	6	8	13	8	0	22	14	14	11	5
Key	v	i	g	e	n	e	r	e	v	i	g	e	n	e	r	e	v	i	g	e	n	e	r	e	v	i
k_i	21	8	6	4	13	4	17	4	21	8	6	4	13	4	17	4	21	8	6	4	13	4	17	4	21	8
c_i	17	15	20	12	5	4	22	21	21	16	9	18	18	25	25	21	1	16	19	12	13	0	5	18	6	13
Ciphertext	r	p	u	m	f	e	w	v	v	q	j	s	s	z	z	v	b	q	t	m	n	a	f	s	g	n

In conclusion, $E(whoisafraidofviginiawoolf) = rpumfewvvqjsszzvbqtmnafsgn$

Use Mathematica to verify my answer:

```
plaintext = "whoisafraidofvirginiawoolf";
key = "vigenere";
ciphertext = "";
Do[ciphertext =
   ciphertext <>             AddTwoLetters[StringTake[plaintext, {i}],
     StringTake[key, {Mod[i - 1, StringLength[key]] + 1}]], {i, 1, StringLength[plaintext]}];
ciphertext
```

```
rpumfewvvqjsszzvbqtmnafsgn
```

Problem Nr.3 *Check that 953 is a prime number and that 3 is a generator of* $Z^*{}_{953}$*. Find the three least significant bits of the solution* m *of the congruence relation* $3^m \equiv 726 \; mod \; 953$*. (See the remark in the discussion of the special case* $q-1=2^n$ *in Subsection 8.3.1.) (08.04)*

Solution.

1) To check 953 is a prime number, I used the mathematica function PrimeQ[].

```
PrimeQ[953]
```

```
True
```

2) If x is a generator or primitive element of finite field GF(p), each nonzero element y in GP(p) can be written as a power of x, such that $y = x^m$, where m is unique modulo p - 1. To check 3 is a generator of $Z^*{}_{953}$, I used the mathematica function PowerList[] from the package "FiniteFields". This function finds a primitive element in F_p and generates all its powers (starting with the 0-th). The second element in this list is the primitive element itself, which means 3 is a generator of $Z^*{}_{953}$

```
<< "FiniteFields`"
```

```
p = 953; PowerList[GF[p, 1]][[2]]
```

```
{3}
```

3) Moreover, to check 3 is a primitive element modulo 953 We know the multiplicative group $Z^*{}_{953}$ has order 952, so each element has an order dividing 952. Since the order of 3 does not divide 952/2, 952/7, 952/17, the order must be 952.

```
FactorInteger[952]
```

```
{{2, 3}, {7, 1}, {17, 1}}
```

```
PowerMod[3, 952 / 2, 953] == 1
PowerMod[3, 952 / 7, 953] == 1
PowerMod[3, 952 / 17, 953] == 1
```

```
False

False

False
```

4) In order to find the solution m of $3^m \equiv 726 \ mod\ 953$, we need to follow these steps:

a. Firstly, we factorize $952 = 2^3 7^1 17^1$, and compute the inverse of 3.

```
In[70]:= q = 953; a = 3; FactorInteger[q - 1]
         x = PowerMod[a, -1, q]

Out[70]= {{2, 3}, {7, 1}, {17, 1}}

Out[71]= 318
```

b. Secondly, we get the corresponding omegas, and a table for omegas' powers.

```
In[72]:= q = 953; a = 3;
         Om1 = PowerMod[a, (q - 1) / 2, q]
         Om2 = PowerMod[a, (q - 1) / 7, q]
         Om3 = PowerMod[a, (q - 1) / 17, q]

Out[73]= 952

Out[74]= 879

Out[75]= 256
         Table[PowerMod[Om1, i, q], {i, 0, 2}]
         Table[PowerMod[Om2, i, q], {i, 0, 7}]
         Table[PowerMod[Om3, i, q], {i, 0, 17}]

Out[97]= {1, 952, 1}

Out[98]= {1, 879, 711, 754, 431, 508, 528, 1}

Out[99]= {1, 256, 732, 604, 238, 889, 770, 802,
          417, 16, 284, 276, 134, 949, 882, 884, 443, 1}
```

c. Thirdly, we use Chinese Remainder Theorem with these factors.

```
In[105]:= u = ChineseRemainder[{1, 0, 0}, {8, 7, 17}]
          v = ChineseRemainder[{0, 1, 0}, {8, 7, 17}]
          w = ChineseRemainder[{0, 0, 1}, {8, 7, 17}]

Out[105]= 833

Out[106]= 680

Out[107]= 392
```

d. Fourthly, we start solving equation $3^m \equiv 726 \; mod \; 953$:

$$q = 953, 952 = 2^3 7^1 17^1, \alpha = 3, \; \alpha^{-1} = 318, c = 726, u = 833, v = 680, w = 392$$

First Prime Factor: $p_1 = 2, n_1 = 3$

$$c = 726, c^{952/2} = 952, m_0 = 1.$$

$$c_1 = c * \alpha^{-1} = 242, {c_1}^{952/4} = 1, m_1 = 0.$$

$$c_2 = c_1 * \alpha^0 = 242, {c_2}^{952/8} = 952, m_2 = 1.$$

Hence : $m^{(1)} = 1 + 0 * 2^1 + 1 * 2^2 = 5.$

Second Prime Factor: $p_2 = 7, n_2 = 1$

$$c = 726, c^{952/7} = 1, m_0 = 0.$$

Hence : $m^{(2)} = 0.$

Third Prime Factor: $p_3 = 17, n_3 = 1$

$$c = 726, c^{952/17} = 256, m_0 = 1.$$

Hence : $m^{(3)} = 1.$

Therefore, the final solution:

$$m = u * m^{(1)} + \; v * m^{(2)} + w * m^{(3)} = 833 * 5 + 680 * 0 + 392 * 1$$

$$= 4557 \equiv 749 \; mod \; 952. \; (3^{749} \equiv 726 \; mod \; 953)$$

Use Mathematica to verify my answer:

```
In[188]:= PowerMod[3, 749, 953]

Out[188]= 726
```

Problem Nr.4 *Check that g = 996 is a generator of the multiplicative group* $Z^*{}_{4007}$*. Set up the index-calculus method with a factor base of size 6 and determine* $log_{996}1111$*. (08.08)*

Solution.

1) To check 4007 is a prime number, I used the mathematica function PrimeQ[]. And to check 996 is a generator, we know $Z^*{}_{4007}$ has order 4006, so each element of the group has an order dividing 4006. Since the order of 996 does not divide 4006/2, 4006/2003, the order must be 4006.

```
In[3]:= p = 4007; PrimeQ[p]
        FactorInteger[p - 1]

Out[3]= True

Out[4]= {{2, 1}, {2003, 1}}

In[5]:= PowerMod[996, 4006 / 2, p]
        PowerMod[996, 4006 / 2003, p]

Out[5]= 4006

Out[6]= 2287
```

2) Use Index-Calculus Method with a factor base of size 6 and calculate $log_{996}1111$.

   a. Firstly, the Factor Base we take is the first 6 prime numbers: {2, 3, 5, 7, 11, 13}.

   b. Secondly, we find 6 elements that can be factorized using the Factor Base.

```
In[391]:= a = 996; p = 4007;
          FactorInteger[PowerMod[a, 8, p]]
          FactorInteger[PowerMod[a, 21, p]]
          FactorInteger[PowerMod[a, 61, p]]
          FactorInteger[PowerMod[a, 65, p]]
          FactorInteger[PowerMod[a, 68, p]]
          FactorInteger[PowerMod[a, 80, p]]

Out[392]= {{2, 5}, {3, 1}}

Out[393]= {{2, 6}, {3, 1}, {11, 1}}

Out[394]= {{3, 2}, {5, 1}, {13, 1}}

Out[395]= {{2, 1}, {3, 2}, {5, 1}, {7, 1}}

Out[396]= {{2, 1}, {3, 1}, {7, 2}, {13, 1}}

Out[397]= {{2, 1}, {5, 2}, {7, 2}}
```

$m_1 = log_{996}2, m_2 = log_{996}3, m_3 = log_{996}5, m_4 = log_{996}7, m_5 = log_{996}11, m_6 = log_{996}13$

For example $996^8 = 996^{5*log_{996}2} * 996^{log_{996}3}\ mod\ 4007, 8 = 5m_1 + m_2\ mod\ 4006$.

We have:

$$8 = 5m_1 + m_2\ mod\ 4006$$

$$21 = 6m_1 + m_2 + m_5\ mod\ 4006$$

$$61 = 2m_2 + m_3 + m_6\ mod\ 4006$$

$$65 = m_1 + 2m_2 + m_3 + m_4\ mod\ 4006$$

$$68 = m_1 + m_2 + 2m_4 + m_6\ mod\ 4006$$

$$80 = m_1 + 2m_3 + 2m_4\ mod\ 4006$$

Moreover, they must be linearly independent:

```
In[452]:= MatrixRank[{{5, 1, 0, 0, 0, 0}, {6, 1, 0, 0, 1, 0}, {0, 2, 1, 0, 0, 1},
            {1, 2, 1, 1, 0, 0}, {1, 1, 0, 2, 0, 1}, {1, 0, 2, 2, 0, 0}}]

Out[452]= 6
```

c. Thirdly, we solve the linearly independent system of equations:

```
In[456]:= m1 =.; m2 =.; m3 =.; m4 =.; m5 =.; m6 =.;
          Solve[{5 * m1 + m2 == 8, 6 * m1 + m2 + m5 == 21, 2 * m2 + m3 + m6 == 61, m1 + 2 * m2 + m3 + m4 == 65,
            m1 + m2 + 2 * m4 + m6 == 68, m1 + 2 * m3 + 2 * m4 == 80}, {m1, m2, m3, m4, m5, m6}, Modulus → 4006]
Out[457]= {{m5 → 1279, m6 → 156, m4 → 1426, m3 → 3253, m2 → 2332, m1 → 2740}}
```

And get:

$$m_1 = log_{996}2 = 2740, m_2 = log_{996}3 = 2332, m_3 = log_{996}5 = 3253,$$

$$m_4 = log_{996}7 = 1426, m_5 = log_{996}11 = 1279,\ m_6 = log_{996}13 = 156.$$

Or, equivalently:

$$996^{2740} \equiv 2\ , 996^{2332} \equiv 3, 996^{3253} \equiv 5, (mod\ 4006),$$

$$996^{1426} \equiv 7, 996^{1279} \equiv 11, 996^{156} \equiv 13, (mod\ 4006).$$

d. Finally, we can find the solution of $996^m \equiv 1111 \; mod \; 4007$, ($m = log_{996} 1111$)

We see that 1111 can not be expressed as product of elements in Factor Base, but $996^1 * 1111$ can.

```
In[374]:= FactorInteger[1111]
          FactorInteger[Mod[996^1 * 1111, 4007]]

Out[374]= {{11, 1}, {101, 1}}

Out[375]= {{2, 4}, {3, 1}, {13, 1}}
```

We conclude that:

$$1 + m = 4 * m_1 + 1 * m_2 + 1 * m_6 = 4 * 2740 + 2332 + 156 \equiv 1430 \; mod \; 4006$$

Therefore, the solution of $996^m \equiv 1111 \; mod \; 4006$ is given by:

$$m \equiv 1429 \; (mod \; 4006)$$

Use Mathematica to Check my solution:

```
In[502]:= PowerMod[996, 1429, 4007]

Out[502]= 1111
```

Problem Nr.5 *Complete Example 9.7. (Hint: extend the search to H-105, 105L.) (09.07)*

Solution.

a. We want to factorize n = 661643, according to the Quadratic Sieve Factoring Algorithm, firstly, we make a Factor Base while the Jacobi Symbol of n and the chosen prime number is 1: {-1, 2, 11, 19, 23, 31, 37, 47, 53, 59, 79, 89}.

```
n = 661643; k = 10;
SS = {-1, 2}; i = 2;
While[Length[SS] - 2 < k,
  If[JacobiSymbol[n, Prime[i]] == 1, AppendTo[SS, Prime[i]]]; i = i + 1];
SS
```

```
Out[68]= {-1, 2, 11, 19, 23, 31, 37, 47, 53, 59, 79, 89}
```

b. Secondly, we choose pairs (a_i, b_i), such that they can be factorized with the Factor Base, while $f(x) = {a_i}^2 - n$ must small numbers:

```
n = 661643; r = ⌊√n⌋;
i = {-74, -55, -52, -39, -34, -2, 4, 10, 41, 69, 72, 100, 104};
a = i + r;
f[x_] := (x + r)^2 - n; b = f[i];
TableForm[Table[ {a[[i]], b[[i]], FactorInteger[ b[[i]] ] // OutputForm}, {i, 1, Length[a]} ],
 TableHeadings → {{}, {"a", "\!\(a\^2\) mod n", "factors"}}, TableAlignments → {Left}]
```

Out[152]//TableForm=

a	a^2 mod n	factors
739	-115522	{{-1, 1}, {2, 1}, {11, 1}, {59, 1}, {89, 1}}
758	-87079	{{-1, 1}, {31, 1}, {53, 2}}
761	-82522	{{-1, 1}, {2, 1}, {11, 3}, {31, 1}}
774	-62567	{{-1, 1}, {19, 1}, {37, 1}, {89, 1}}
779	-54802	{{-1, 1}, {2, 1}, {11, 1}, {47, 1}, {53, 1}}
811	-3922	{{-1, 1}, {2, 1}, {37, 1}, {53, 1}}
817	5846	{{2, 1}, {37, 1}, {79, 1}}
823	15686	{{2, 1}, {11, 1}, {23, 1}, {31, 1}}
854	67673	{{31, 1}, {37, 1}, {59, 1}}
882	116281	{{11, 2}, {31, 2}}
885	121582	{{2, 1}, {31, 1}, {37, 1}, {53, 1}}
913	171926	{{2, 1}, {31, 1}, {47, 1}, {59, 1}}
917	179246	{{2, 1}, {19, 1}, {53, 1}, {89, 1}}

c. Thirdly, we conclude the exponents in the factorization of $b_i's$ to form a matrix U, and use modulo 2 reductions to form a matrix V.

```
In[171]:= U = {{1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1}, {1, 0, 0, 0, 0, 1, 0, 0, 2, 0, 0, 0},
             {1, 1, 3, 0, 0, 1, 0, 0, 0, 0, 0, 0}, {1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1},
             {1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0}, {1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0},
             {0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0}, {0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0},
             {0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0}, {0, 2, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0},
             {0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0}, {0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0},
             {0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0}};
         V = Mod[U, 2];
         MatrixForm[V]
```

Out[173]//MatrixForm=

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

d. Fourthly, we find a non-trivial linear combination of the rows of V adding up to the all-zero vector modulo 2 and get a solution (the first one).

```
In[157]:= NullSpace[Transpose[V], Modulus → 2]

Out[157]= {{0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0}, {0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0}, {0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0}}
```

e. Finally, we get x and y respectively using the above solution, and the factor will be the greatest common divisor of $x - y$ and n:

```
In[163]:= x = a[[2]] * a[[3]] * a[[5]] * a[[6]] * a[[9]] * a[[12]]
          y = (b[[2]] * b[[3]] * b[[5]] * b[[6]] * b[[9]] * b[[12]])^(1/2)
          GCD[x - y, n]

Out[163]= 284 145 526 155 966 244

Out[164]= 134 051 624 754 916

Out[165]= 1223
```

$$such\ that: n = 661643 = 1223 * 541$$

```
In[166]:= n / 1223

Out[166]= 541
```

Problem Nr.6 *Suppose that Alice has sent secret messages $m_1 = m$, $m_2 = m^2 + 10m + 20$ to Bob by the RSA system. Let Bob's modulus be $n_B = 483047$ and $e_B = 3$. Suppose that you have intercepted the transmitted ciphertexts $c_1 = 346208$ resp. $c_2 = 230313$ and that you know the above relation between m1 and m2. Determine m1 (see Example 9.10). (09.11)*

Solution.

a. Firstly, according to the General Method through GCD calculation, the message can be recovered by $gcd(z^e - c_1, f(z)^e - c_2)\ mod\ n_B$, however, $n_B = 483047$ is not prime, we need to compute the gcd step by step using Euclid's Algorithm:

```
In[183]:= PrimeQ[483047]

Out[183]= False
```

b. We have: $f_1(z) = z^6 + 30z^5 + 360z^4 + 2200z^3 + 7200z^2 + 12000z + 260734$

and $f_2(z) = z^3 - 346208$ over $Z_{483047}[z]$.

Start Euclid's Algorithm:

$$f_1(z) = f_2(z)(z^3 + 30z^2 + 360z + 348408) + (249453z^2 + 20754z + 231228)$$

$$f_2(z) = f_3(z)(21839z + 132325) + (317238z + 54813)$$

$$f_3(z) = f_4(z)(351887z + 172538) + (0)$$

So $gcd(f_1(z), f_2(z)) = 317238z + 54813$

```
In[269]:= n = 483047; c1 = 346208; c2 = 230313;
          f1 = Expand[(z^2 + 10 z + 20)^3 - c2]
          f2 = z^3 - c1;
          f3 = PolynomialMod[f1 - f2 * (z^3 + 30 z^2 + 360 z + 348408), n]

Out[270]= -222313 + 12000 z + 7200 z^2 + 2200 z^3 + 360 z^4 + 30 z^5 + z^6

Out[272]= 231228 + 20754 z + 249453 z^2

In[273]:= f4 = PolynomialMod[f2 - f3 * (21839 z + 132325), n]

Out[273]= 54813 + 317238 z

In[274]:= f5 = PolynomialMod[f3 - f4 * (351887 z + 172538), n]

Out[274]= 0
```

```
In[275]:= InverseLeadCoeff = PowerMod[317238, -1, n];
          f4 = PolynomialMod[InverseLeadCoeff * f4, n]

Out[276]= 50947 + z
```

c. Moreover:

$$gcd(f_1(z), f_2(z)) \equiv 317238z + 54813 \equiv$$

$$\equiv z + 50947 \equiv z - 432100 \; (mod\; 483047)$$

Therefore, the secrete message m is 432100.

d. Use Mathematica to verify my answer:

```
In[282]:= m = 432100; n = 483047;
          PowerMod[m, 3, n] == c1
          PowerMod[m^2 + 10 m + 20, 3, n] == c2

Out[283]= True

Out[284]= True
```

Problem Nr.7 *Let (G, *) denote a commutative group. Let a and b be two elements in G of order m resp. n. (a) Assume that gcd(m, n) = 1. Show that a * b has order m * n. (b) Assume no longer that gcd(m, n) = 1. Determine integers s and t such that s | m, t | n, gcd(s, t) = 1, and lcm[s, t] = lcm[m, n]. (c) Construct an element in G of order lcm[m, n]. (B.06)*

Solution.

a. Since a, b commute, then we have $(ab)^{mn} = a^{mn}b^{mn} = e$, where e is the identity element in G, this means o(ab)|mn, where o(ab) is the order of ab in G. Now, suppose o(ab) = r, such that $(ab)^r = e$. Raising m to both sides, we have $(ab)^{rm} = b^{rm} = e$, means that n|rm. Since gcd(m,n) = 1, we have n|r. Similarly, (by raising n to both sides), we will have m|r. Now we have n|r and m|r, since gcd(m,n) = 1, we will have mn|o(ab), means that o(ab) = mn.

b. Since gcd(s, t)=1, as we know the least common multiple of two integers is the product divided by the gcd, which means that lcm(s, t) = st/gcd(s, t) = st/1 = st. This yields to st = lcm(m, n). For example, if m = 4, n = 6, lcm = 12, and st = 12, s|4, t|6. Then s=4 while t=3, or s=2 while t=6.

c. Two cases for this item:

   a) For the case gcd(m, n) = 1, from item a, we know ab has order mn, and lcm(m, n) = mn/gcd(m, n) = mn, which means ab is the element has order lcm(m, n) that we want to construct.

   b) For the case gcd(m, n) ≠ 1, we write lcm(m, n) = $p_1^{r_1} \dots p_s^{r_s}$ for distinct primes p_i and corresponding orders r_i. If we could find an element in G with order $p_i^{r_i}$ for every i, then the product of these elements will have order lcm(m, n) because prime powers are all relatively prime to prime powers of different primes. Let i with $1 \le i \le s$ be given. We note that $p_i^{r_i}$ divides either m or n. Thus $a^{m/p_i^{r_i}}$ or $b^{n/p_i^{r_i}}$ (whichever one divides evenly) has order $p_i^{r_i}$. Therefore, the products of these elements is the element of order lcm(m, n).

Problem Nr.8 *Let α in GF(q) have order m, m < q - 1. What is the probability that a random non-zero element β in GF(q) has an order n dividing m? Give an upperbound on this probability. Construct an element of order lcm[m, n] (hint: see Problem B.06). (In fact, this method leads to an efficient to find a primitive element in a finite field. It is due to Gauss.) (B.10)*

Solution.

In order to solve this problem, we will use the following theorems:

Definition A.6
The *Euler's Totient Function* ϕ (see Euler) is defined by

$$\phi(m) = |\{ 0 \le i < m \mid \gcd(i, m) = 1 \}|.$$

In words, $\phi(m)$ is the number of integers in between 0 and $m - 1$ that are coprime with m.

Theorem A.12
For all positive integers m

$$\textstyle\sum_{d|m} \varphi(d) = m.$$

Proof of Theorem A.12:

Let d divide m. By writing $r = i\,d$ one sees immediately that the number of elements r, $0 \le r < m$, with $\gcd(r, m) = d$ is equal to the number of integers i with $0 \le i < \frac{m}{d}$ and $\gcd(i, \frac{m}{d}) = 1$, therefore, this number is $\phi(\frac{m}{d})$.

On the other hand, $\gcd(r, m)$ divides n for each integer r, $0 \le r < m$. It follows that $\sum_{d|m} \phi(\frac{m}{d}) = m$. This statement is equivalent to what needs to be proved.

Theorem B.5
Let $(G, \cdot)$ be a finite group of order n. Then every subgroup $(H, \cdot)$ of $(G, \cdot)$ has an order dividing n. Also every element a, $a \ne e$, in G has an order dividing n.

Theorem B.21
Let $(\mathbb{F}_q, +, \cdot)$ be a finite field and let d be an integer dividing $q - 1$. Then $\mathbb{F}_q$ contains exactly $\phi(d)$ elements of order d.
In particular, $(\mathbb{F}_q \setminus \{0\}, \cdot)$ is a cyclic group of order $q - 1$, which contains $\phi(q - 1)$ primitive elements.

Proof: By Theorem B.5, every non-zero element in $\mathbb{F}_q$ has a multiplicative order d, which divides $q-1$. On the other hand, suppose that $\mathbb{F}_q$ contains an element of order d, $d \mid (q-1)$, say ω. Then all d distinct powers of ω are a zero of $x^d - e$. It follows from Theorem B.15 that every d-th root of unity in $\mathbb{F}_q$ is a power of ω. It follows from Lemma B.4 that under the assumption that $\mathbb{F}_q$ contains an element of order d, $\mathbb{F}_q$ will contain exactly $\phi(d)$ elements of order d, namely ω^i, with $\mathrm{GCD}[i, d] = 1$.

Let $a(d)$ be the number of elements of order d in $\mathbb{F}_q$. Then the above implies that

i) $a(d) = 0$ or $a(d) = \phi(d)$

and also that

ii) $\sum_{d|(q-1)} a(d) = q-1$.

On the other hand, Theorem A.12 states that $\sum_{d|(q-1)} \phi(d) = q-1$. So, we conclude that $a(d) = \phi(d)$ for all $d \mid (q-1)$.

In particular, $a(q-1) = \phi(q-1)$ which means that $\mathbb{F}_q$ contains $\phi(q-1)$ primitive elements and that $\mathbb{F}_q \setminus \{0\}$ is a cyclic group.

1) α in GF(q) has order m < q - 1, we want to know the number of elements β in GF(q) such that, o(β) = n, n|m.

Case 1: m|(q - 1) and m is prime. Then, there exists a subgroup in GF(q) with exactly m elements, and all the elements β's in this subgroup have a order dividing m, thus the probability is

$$\frac{|\beta's|}{|GF(q)|} = \frac{m}{q-1}$$

Case 2: m|(q - 1) but m is not a prime, then by factoring m = $p_1^{r_1} \dots p_s^{r_s}$, the β's we want are the elements having the order of these factors. Since o(β) = n, n|m, n|q, the number of β's with order n is $\phi(n)$ by Theorem B.21. Then, for all β's with order dividing m, the number is $\sum_{n|m} \phi(n)$, by Theorem A.12, that is m. So the probability is

$$\frac{|\beta's|}{|GF(q)|} = \frac{m}{q-1}$$

Case 3: m does not divide (q - 1). We consider gcd(m, q - 1), similar with the above two cases, the probability is:

$$\frac{|\beta's|}{|GF(q)|} = \frac{gcd(m, q-1)}{q-1}$$

In conclusion, the upper bound of the probability is $m/_{q-1}$.

2) If n|m, lcm(m, n) = m, then element of order lcm(m, n) is α itself.

If n does not divide m, probability is $(1 - {}^{m}/_{q-1})$, from B.06, we have 2 cases:

a) For the case gcd(m, n) = 1, we know $\alpha\beta$ has order mn, and lcm(m, n) = mn/gcd(m, n) = mn, which means $\alpha\beta$ is the element has order lcm(m, n) that we want to construct.

b) For the case gcd(m, n) ≠ 1, we write lcm(m, n) $= p_1^{r_1} \ldots p_s^{r_s}$ for distinct primes p_i and corresponding orders r_i. If we could find an element in GF(q) with order $p_i^{r_i}$ for every i, then the product of these elements will have order lcm(m, n) because prime powers are all relatively prime to prime powers of different primes. Let i with $1 \leq i \leq s$ be given. We note that $p_i^{r_i}$ divides either m or n. Thus $a^{m/p_i^{r_i}}$ or $b^{n/p_i^{r_i}}$ (whichever one divides evenly) has order $p_i^{r_i}$. Therefore, the products of these elements is the element of order lcm(m, n).

c) Moreover, the element will be the primitive element of GF(q).

3) Guass procedure to find a primitive element:

```
Choose a non-zero element α in GF(q).
Let m := o(α), m is the first power of α such that α^m = 1.
If m = q - 1:
     Output("α is primitive"), and finish.
Else:
     While α is not primitive:
          Find β, whose order IS NOT a divisor of m,
          Update α = αβ, and m = lcm(m, n),
          Output("α is primitive"), and finish.
```

Problem Nr.9 *Duplicate Example 10.6 for the elliptic curve* Ɛ *over* Z_{523} *defined by the equation* $y^2 = x^3 + 111x^2 + 11x + 1$. *Use for P a point of order at least one hundred. (10.07)*

Solution.

a. For the elliptic curve Ɛ over Z_{523}, the point P = {1, 80} lies on it:

```
In[23]:= p = 523; a = 111; b = 11; c = 1;

In[74]:= x = 1; y = 80; Mod[y^2 - (x^3 + a*x^2 + b*x + c), p] == 0

Out[74]= True
```

b. The point P = {1, 80} has order 528 since it goes to zero after 528 additions:

```
In[257]:= Clear[f];
          p = 523; a = 111; b = 11; c = 1; P = {1, 80}; f[1] = P;
          f[n_] := f[n] = EllipticAdd[p, a, b, c, P, f[n - 1]];
          Table[f[i], {i, 528 - 1, 528 + 1}]

Out[260]= {{1, 443}, {O}, {1, 80}}
```

c. Moreover, only $528 * P = O$, while other factors of 528 do not(We convert integers into binary representation first, and use $EllipticAdd()$ with corresponding indexes $P[i]$):

```
In[445]:= FactorInteger[528]
          IntegerDigits[528, 2]
          IntegerDigits[528 / 2, 2]
          IntegerDigits[528 / 3, 2]
          IntegerDigits[528 / 11, 2]

Out[445]= {{2, 4}, {3, 1}, {11, 1}}

Out[446]= {1, 0, 0, 0, 0, 1, 0, 0, 0, 0}

Out[447]= {1, 0, 0, 0, 0, 1, 0, 0, 0}

Out[448]= {1, 0, 1, 1, 0, 0, 0, 0}

Out[449]= {1, 1, 0, 0, 0, 0}
```

```
In[450]:= Clear[P];
          p = 523; P =.;
          a = 111; b = 11; c = 1;
          P[0] = {1, 80};
          P[i_] := P[i] = EllipticAdd[p, a, b, c, P[i - 1], P[i - 1]];
          Q = EllipticAdd[p, a, b, c, P[9], P[4]]
          EllipticAdd[p, a, b, c, P[8], P[3]]
          EllipticAdd[p, a, b, c, P[7], EllipticAdd[p, a, b, c, P[5], P[4]]]
          EllipticAdd[p, a, b, c, P[5], P[4]]

Out[455]= {O}

Out[456]= {195, 0}

Out[457]= {174, 165}

Out[458]= {32, 226}
```

d. Then let Alice choose $m_A = 130$, and Bob choose $m_B = 288$, then:

$$Q_A = (332, 414), and\ Q_B = (49, 214)$$

```
In[463]:= IntegerDigits[130, 2]
          IntegerDigits[288, 2]

Out[463]= {1, 0, 0, 0, 0, 0, 1, 0}

Out[464]= {1, 0, 0, 1, 0, 0, 0, 0, 0}

In[465]:= QAlice = EllipticAdd[p, a, b, c, P[7], P[1]]
          QBob = EllipticAdd[p, a, b, c, P[8], P[5]]

Out[465]= {332, 414}

Out[466]= {49, 214}
```

(Use $EllipticAdd()$ with corresponding indexes $P[i]$)

e. Finally, compute the common key $K_{A,B}$:

$$\text{Alice: } K_{A,B} = m_A Q_B = (32, 297)$$

$$\text{Bob: } K_{A,B} = m_A Q_A = (32, 297)$$

```
In[467]:= Clear[QA]; QA[0] = {49, 214};
          QA[i_] := QA[i] = EllipticAdd[p, a, b, c, QA[i - 1], QA[i - 1]];
          EllipticAdd[p, a, b, c, QA[7], QA[1]]

Out[469]= {32, 297}
```

```
In[470]:= Clear[QB]; QB[0] = {332, 414};
          QB[i_] := QB[i] = EllipticAdd[p, a, b, c, QB[i - 1], QB[i - 1]];
          EllipticAdd[p, a, b, c, QB[8], QB[5]]

Out[472]= {32, 297}
```

As expected, they have the same results.

Problem Nr.10 *Consider the following scheme over Z_3 :*

Participant	*Share*
1	$a, b, c + s_2$
2	$a + s_1, b, c$
3	$b + s_1, c - s_2, d$
4	$b, d + s_2,$

Give the matrix description of this scheme. Prove that it is a secret sharing scheme for access structure (U, P, N) with U = {1, 2, 3, 4}, P = {{1, 2}, {2, 3}, {3, 1}, {3, 4}} and N = {{1, 4}, {2, 4}, {3}}. What is the information rate of this scheme? Is it perfect? Is it ideal? (15.04)

Solution.

1) Matrix description of this scheme (The first two columns are labeled by the secret bits s_1, s_2, and the next four columns by the random variables a, b, c, d):

In[16]:= $GTA = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$; $Gp1 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$;

$Gp2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$; $Gp3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$; $Gp4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$;

```
In[9]:= Clear[a, b, c, d, s1, s2];
vec = {s1, s2, a, b, c, d};
GTA.vec
Gp1.vec
Gp2.vec
Gp3.vec
Gp4.vec

Out[11]= {s1, s2}

Out[12]= {a, b, c + s2}

Out[13]= {a + s1, b, c}

Out[14]= {b + s1, c - s2, d}

Out[15]= {b, d + s2}
```

2) Verify the secrets (Privileged Sets *P = {{1, 2}, {2, 3}, {3, 1}, {3, 4}}* can recover secrets s_1, s_2, while Non-Privileged Sets *N = {{1, 4}, {2, 4}, {3}}* can not):

{1, 2} recover s_1:

```
In[40]:= Clear[u, M];
         u = GTA⟦1⟧;
         M = Join[Gp1, Gp2]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

Out[43]= {2, 0, 0, 1, 0, 0}
```

{1, 2} recover s_2:

```
In[44]:= Clear[u, M];
         u = GTA⟦2⟧;
         M = Join[Gp1, Gp2]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

Out[47]= {0, 0, 1, 0, 0, 2}
```

{2, 3} recover s_1:

```
In[48]:= Clear[u, M];
         u = GTA⟦1⟧;
         M = Join[Gp2, Gp3]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

Out[51]= {0, 2, 0, 1, 0, 0}
```

{2, 3} recover s_2:

```
In[52]:= Clear[u, M];
         u = GTA⟦2⟧;
         M = Join[Gp2, Gp3]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

Out[55]= {0, 0, 1, 0, 2, 0}
```

{3, 1} recover s_1:

```
In[56]:= Clear[u, M];
         u = GTA[[1]];
         M = Join[Gp3, Gp1]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

Out[59]= {1, 0, 0, 0, 2, 0}
```

{3, 1} recover s_2:

```
In[60]:= Clear[u, M];
         u = GTA[[2]];
         M = Join[Gp3, Gp1]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

ut[63]= {0, 1, 0, 0, 0, 2}
```

{3, 4} recover s_1:

```
In[64]:= Clear[u, M];
         u = GTA[[1]];
         M = Join[Gp3, Gp4]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

Out[67]= {1, 0, 0, 2, 0}
```

{3, 4} recover s_2:

```
In[68]:= Clear[u, M];
         u = GTA[[2]];
         M = Join[Gp3, Gp4]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

Out[71]= {0, 0, 2, 0, 1}
```

$\{1, 4\}$ can not recover s_1:

```
In[72]:= Clear[u, M];
         u = GTA[[1]];
         M = Join[Gp1, Gp4]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

         ··· LinearSolve: Linear equation encountered that has no solution.

Out[75]= LinearSolve[{{0, 0, 0, 0, 0}, {0, 0, 1, 0, 1}, {1, 0, 0, 0
```

$\{1, 4\}$ can not recover s_2:

```
In[76]:= Clear[u, M];
         u = GTA[[2]];
         M = Join[Gp1, Gp4]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

         ··· LinearSolve: Linear equation encountered that has no solution.

Out[79]= LinearSolve[{{0, 0, 0, 0, 0}, {0, 0, 1, 0, 1}, {1, 0, 0,
```

$\{2, 4\}$ can not recover s_1:

```
In[80]:= Clear[u, M];
         u = GTA[[1]];
         M = Join[Gp2, Gp4]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

         ··· LinearSolve: Linear equation encountered that has no solution.

Out[83]= LinearSolve[{{1, 0, 0, 0, 0}, {0, 0, 0, 0, 1}, {1, 0, 0,
```

$\{2, 4\}$ can not recover s_2:

```
In[84]:= Clear[u, M];
         u = GTA[[2]];
         M = Join[Gp2, Gp4]; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

         ··· LinearSolve: Linear equation encountered that has no solution.

Out[87]= LinearSolve[{{1, 0, 0, 0, 0}, {0, 0, 0, 0, 1}, {1, 0, 0,
```

{3} can not recover s_1:

```
In[88]:= Clear[u, M];
         u = GTA[[1]];
         M = Gp3; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

         ••• LinearSolve: Linear equation encountered that has no solution.

Out[91]= LinearSolve[{{1, 0, 0}, {0, -1, 0}, {0, 0, 0}, {1, 0, 0},
```

{3} can not recover s_2:

```
In[92]:= Clear[u, M];
         u = GTA[[2]];
         M = Gp3; MatrixForm[M];
         LinearSolve[Transpose[M], u, Modulus → 3]

         ••• LinearSolve: Linear equation encountered that has no solution.

Out[95]= LinearSolve[{{1, 0, 0}, {0, -1, 0}, {0, 0, 0}, {1, 0, 0},
```

3) The information rare is the ratio between the size of the secret and the size of the longest share, so in this case is 2/3.

4) The scheme is called perfect if the shares of any authorized subset uniquely determine the value of the secret, and the shares of a non-authorized subset give no information about the secret. From the experiments I made in item (1), the scheme is perfect.

5) A more compact way to denote this secret sharing scheme is:

Participant	*Share*
1	$a_1{}^{\{1,2\}}, a_1{}^{\{2,3\}}, a_1{}^{\{3,1\}} + s_2$
2	$a_1{}^{\{1,2\}} + s_1, a_1{}^{\{2,3\}}, a_1{}^{\{3,1\}}$
3	$a_1{}^{\{2,3\}} + s_1, a_1{}^{\{3,1\}} - s_2, a_1{}^{\{3,4\}}$
4	$a_1{}^{\{2,3\}}, a_1{}^{\{3,4\}} + s_2,$

A perfect scheme is called ideal if it has an efficiency rate equal to 1, so our case is not ideal.