TD4

## Arithmetic

### Exercice 1

1. u0 = 1

v0 = 0

u1 = 0

v1 = 1

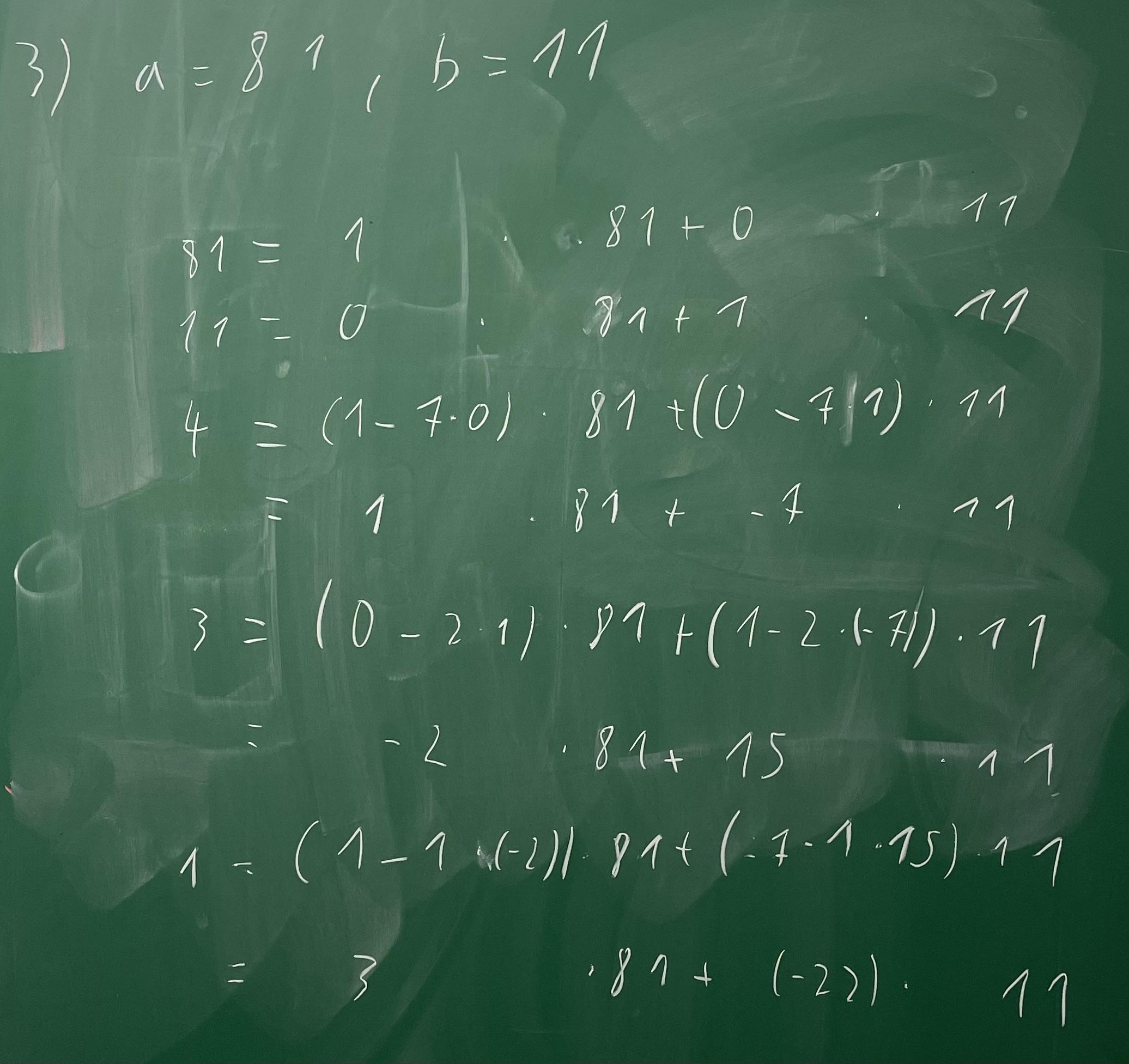
a=r0=u0a+v0b

b=r1=u1a+v1b

donc :

1. a=81, b=11

| i | r | u | v | q |
| --- | --- | --- | --- | --- |
| 0 | 81 | 1 | 0 | 7 |
| 1 | 11 | 0 | 1 | 2 |
| 2 | 4 | 1 | -7 | 1 |
| 3 | 3 | -2 | 15 | 3 |
| 4 | 1 | 3 | -22 | impossible |
| 5 | 0 | -11 | 81 |  |



1. a\*b modulo N =1

b est inverse de a modulo N

1 = 3\*81 +(-22)\*11

1=3\*81 mod N

donc 3 est l’inverse de 81 modulo 11

### Exercice 2

p=19;q=23

1. N=pq=437

ϕ(N)=(p-1)(q-1)=396

1. de = 1 (mod ϕ(N)) (le modulo s’applique sur toute l’équation)

d.5 = 1+k\*396

1= d\*5+z\*396

r0 = 396 r2=396- [396/5]\*5 = 1 = 396\*1 - 79 \* 5

r1=5

r3= 5-[5/1]\*1 = 0

donc d=-79=317

Pour e=9, ce n’est pas possible car 9 et 396 ne sont pas premiers entre eux.

1. m=42

c=m^e mod N

c=42^5 mod 437

c=264

Vérification

264^317 mod 437 = 42

### Exercice 3

1. Comme N\_A=N\_B, on a p\_A=p\_B et q\_A=q\_B et phi(N\_A)=phi(N\_B).

Bob peut donc calculer d\_A et déchiffrer un message destiné à Alice.

1. On a:

c\_A=m^(e\_A) mod N

c\_B=m^(e\_B) mod N

Comme e\_A et e\_B sont premier entre eux, on peut calculer u\_A et u\_B tel que :

1 = u\_A\*e\_A+u\_B\*e\_B

c\_A^(u\_A)\*c\_B^(u\_B)

= (m^(e\_A))^(u\_A)\*(m^(e\_B))^(u\_B) mod N

= m^(e\_A\*u\_A)\*m^(e\_B\*u\_B) mod N

= m^(e\_A\*u\_A+e\_B+u\_B) mod N

= m^1 mod N

### Exercice 4

1. Ks=b

Kp=g^b

c=(g^k,K\_p^k\*m)=c(g^k,g^bk\*m)

(u^b)^-1

=((g^k)^b)^-1\*g^(bk)\*m

=m

1. c=(g^k,k\_p^k\*m),m,Kr,c’=(g^k,k\_p^k\*m’)

On peut trouver m’ comme suit :

On calcule (v\*m^-1)^-1\*v’=m’

Car (v\*m^-1)^-1\*v’=(kr^k)^-1\*k\_r^k\*m’

=m

1. Soit c\_1=(u\_1,v\_1)=(g^k1),k\_p^k1\*m1)

c\_2=(u2,v\_2)=(g^k2,k\_p^k2\*m2)

Soit c\_1\*c\_2=(u\_1\*u\_2,v\_1\*v\_2)

Donc ElGamal est malléable