

## Briser les symétries, Denise Vella-Chemla, 15 octobre 2024

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

On présente ici les résultats d'un programme python qui semblent permettre de distinguer de façon sûre les nombres qui sont des décomposants de Goldbach d'un nombre pair  $n$  des nombres qui n'en sont pas.

On rappelle le petit théorème de Fermat :

*Soit  $p$  un nombre premier et soit  $a \in \mathbb{N}$ .*

*Si  $a$  est premier à  $p$  ( $\text{pgcd}(a, p) = 1$ ) alors  $a^{p-1} \equiv 1 \pmod{p}$ .*

On décide de tester par programme les puissances intervenant dans le petit théorème de Fermat, de façon systématique, pour trois nombres qui sont particularisés par l'énoncé de la conjecture de Goldbach : ces nombres sont :

- d'une part  $a$  et  $b$ , avec  $a$  un nombre impair inférieur à la moitié de  $n$ , le nombre pair à décomposer, et  $b$ , son complémentaire à  $n$  :  $b = n - a$  ;
- d'autre part,  $c$  le nombre égal à la moitié de  $n$  puisque  $n$  est pair.

On calcule les valeurs :

- des puissances  $b^{a-1}$  et  $c^{a-1}$  dans  $\mathbb{Z}/a\mathbb{Z}$  ;
- des puissances  $a^{b-1}$  et  $c^{b-1}$  dans  $\mathbb{Z}/b\mathbb{Z}$  ;
- et des puissances  $a^{c-1}$  et  $b^{c-1}$  dans  $\mathbb{Z}/c\mathbb{Z}$ .

On constate, ce qui découle du petit théorème de Fermat, que pour  $n$ , un nombre pair double d'un nombre composé : si 4 au moins des 6 puissances calculées ci-dessus sont égales à 1, et si les 2 seules puissances différentes de 1 (parmi les 6) sont les puissances  $a^{b-1}$  et  $c^{b-1}$ , ( $b-1$  est composé) alors  $a$  et  $b$  sont deux nombres premiers, i.e.  $n = a + b$  est une décomposition de Goldbach de  $n$ .

Il faudrait être capable de démontrer que deux nombres vérifiant toutes ces contraintes existent toujours quel que soit  $n$ .

Pour résumer, on cherche à savoir s'il existe toujours un nombre  $x$  impair compris entre 3 et  $\frac{n}{2}$  tel que :

$$\left\{ \begin{array}{l} x^{\left(\frac{n}{2}-1\right)} \not\equiv 1 \pmod{\frac{n}{2}} \\ (n-x)^{\left(\frac{n}{2}-1\right)} \not\equiv 1 \pmod{\frac{n}{2}} \\ \left(\frac{n}{2}\right)^{x-1} \equiv 1 \pmod{x} \\ (n-x)^{(x-1)} \equiv 1 \pmod{x} \\ x^{(n-x-1)} \equiv 1 \pmod{n-x} \\ \left(\frac{n}{2}\right)^{n-x-1} \equiv 1 \pmod{n-x} \end{array} \right.$$

car ceci est la caractérisation par le petit théorème de Fermat du fait que  $x$  et  $n - x$  sont premiers et fournissent une décomposition de Goldbach de  $n$ .

On remarque également par programme qu'il existe quasiment toujours une décomposition de Goldbach  $x + (n - x)$  de  $n$  telle que  $n - x$  est une racine primitive de  $x$  mais cela ne nous permet pas de fournir une explication de l'existence obligatoire d'une décomposition de Goldbach pour autant car les congruences ont lieu dans trois anneaux différents que l'on ne parvient pas à relier.

## Annexe 1 : texte python du programme

```
def prime(atester):
    k = 2
    if atester in [0, 1]: return False
    if atester in [2, 3, 5, 7]: return True
    while True:
        if k * k > atester: return True
        else:
            if atester % k == 0: return False
            else: k = k + 1

for n in range(6,104,2):
    if not prime(n/2):
        print('::::::::::::',n)
        print('les dg ')
        for x in range(3,n//2+2,2):
            if prime(x) and prime(n-x):
                print(x,' --> ')
                a = x
                b = n//2
                c = n-x
                print(b,'b**(a-1) mod a ',(b**(a-1))%a)
                print(c,'c**(a-1) mod a ',(c**(a-1))%a)
                print(a,'a**(b-1) mod b ',(a**(b-1))%b)
```

```

        print(c,'c**(b-1) mod b ',(c**(b-1))%b)
        print(a,'a**(c-1) mod c ',(a**(c-1))%c)
        print(b,'b**(c-1) mod c ',(b**(c-1))%c)
print('non dg ')
for x in range(3,n//2+2,2):
    if not prime(x) or not prime(n-x):
        print(x,' --> ')
        a = x
        b = n//2
        c = n-x
        print(b,'b**(a-1) mod a
',(b**(a-1))%a)
        print(c,'c**(a-1) mod a ',(c**(a-1))%a)
        print(a,'a**(b-1) mod b ',(a**(b-1))%b)
        print(c,'c**(b-1) mod b ',(c**(b-1))%b)
        print(a,'a**(c-1) mod c ',(a**(c-1))%c)
        print(b,'b**(c-1) mod c ',(b**(c-1))%c)

```

## Annexe 2 : calcul des 6 puissances pour les nombres pairs doubles d'un nombre composé

```

:.....: 8
les dg
3 -->
4 b**(a-1) mod a 1
5 c**(a-1) mod a 1
3 a**(b-1) mod b 3
5 c**(b-1) mod b 1
3 a**(c-1) mod c 1
4 b**(c-1) mod c 1
5 -->
4 b**(a-1) mod a 1
3 c**(a-1) mod a 1
5 a**(b-1) mod b 1
3 c**(b-1) mod b 3
5 a**(c-1) mod c 1
4 b**(c-1) mod c 1
les non dg

:.....: 12
les dg
5 -->
6 b**(a-1) mod a 1
7 c**(a-1) mod a 1
5 a**(b-1) mod b 5
7 c**(b-1) mod b 1
5 a**(c-1) mod c 1
6 b**(c-1) mod c 1

```

```

7 -->
6 b**(a-1) mod a 1
5 c**(a-1) mod a 1
7 a**(b-1) mod b 1
5 c**(b-1) mod b 5
7 a**(c-1) mod c 1
6 b**(c-1) mod c 1
les non dg
3 -->
6 b**(a-1) mod a 0
9 c**(a-1) mod a 0
3 a**(b-1) mod b 3
9 c**(b-1) mod b 3
3 a**(c-1) mod c 0
6 b**(c-1) mod c 0
::: 16
les dg
3 -->
8 b**(a-1) mod a 1
13 c**(a-1) mod a 1
3 a**(b-1) mod b 3
13 c**(b-1) mod b 5
3 a**(c-1) mod c 1
8 b**(c-1) mod c 1
5 -->
8 b**(a-1) mod a 1
11 c**(a-1) mod a 1
5 a**(b-1) mod b 5
11 c**(b-1) mod b 3
5 a**(c-1) mod c 1
8 b**(c-1) mod c 1
les non dg
7 -->
8 b**(a-1) mod a 1
9 c**(a-1) mod a 1
7 a**(b-1) mod b 7
9 c**(b-1) mod b 1
7 a**(c-1) mod c 4
8 b**(c-1) mod c 1
9 -->
8 b**(a-1) mod a 1
7 c**(a-1) mod a 4
9 a**(b-1) mod b 1
7 c**(b-1) mod b 7
9 a**(c-1) mod c 1
8 b**(c-1) mod c 1

```

.....: 18

les dg

5 -->

9  $b^{**}(a-1) \bmod a$  1

13  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  7

13  $c^{**}(b-1) \bmod b$  7

5  $a^{**}(c-1) \bmod c$  1

9  $b^{**}(c-1) \bmod c$  1

7 -->

9  $b^{**}(a-1) \bmod a$  1

11  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  4

11  $c^{**}(b-1) \bmod b$  4

7  $a^{**}(c-1) \bmod c$  1

9  $b^{**}(c-1) \bmod c$  1

les non dg

3 -->

9  $b^{**}(a-1) \bmod a$  0

15  $c^{**}(a-1) \bmod a$  0

3  $a^{**}(b-1) \bmod b$  0

15  $c^{**}(b-1) \bmod b$  0

3  $a^{**}(c-1) \bmod c$  9

9  $b^{**}(c-1) \bmod c$  6

9 -->

9  $b^{**}(a-1) \bmod a$  0

9  $c^{**}(a-1) \bmod a$  0

9  $a^{**}(b-1) \bmod b$  0

9  $c^{**}(b-1) \bmod b$  0

9  $a^{**}(c-1) \bmod c$  0

9  $b^{**}(c-1) \bmod c$  0

.....: 20

les dg

3 -->

10  $b^{**}(a-1) \bmod a$  1

17  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  3

17  $c^{**}(b-1) \bmod b$  7

3  $a^{**}(c-1) \bmod c$  1

10  $b^{**}(c-1) \bmod c$  1

7 -->

10  $b^{**}(a-1) \bmod a$  1

13  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  7

13  $c^{**}(b-1) \bmod b$  3

7  $a^{**}(c-1) \bmod c$  1

10  $b^{**}(c-1) \bmod c$  1

les non dg

5 -->

10  $b^{**}(a-1) \bmod a$  0  
15  $c^{**}(a-1) \bmod a$  0  
5  $a^{**}(b-1) \bmod b$  5  
15  $c^{**}(b-1) \bmod b$  5  
5  $a^{**}(c-1) \bmod c$  10  
10  $b^{**}(c-1) \bmod c$  10

9 -->

10  $b^{**}(a-1) \bmod a$  1  
11  $c^{**}(a-1) \bmod a$  4  
9  $a^{**}(b-1) \bmod b$  9  
11  $c^{**}(b-1) \bmod b$  1  
9  $a^{**}(c-1) \bmod c$  1  
10  $b^{**}(c-1) \bmod c$  1

11 -->

10  $b^{**}(a-1) \bmod a$  1  
9  $c^{**}(a-1) \bmod a$  1  
11  $a^{**}(b-1) \bmod b$  1  
9  $c^{**}(b-1) \bmod b$  9  
11  $a^{**}(c-1) \bmod c$  4  
10  $b^{**}(c-1) \bmod c$  1

.....: 24

les dg

5 -->

12  $b^{**}(a-1) \bmod a$  1  
19  $c^{**}(a-1) \bmod a$  1  
5  $a^{**}(b-1) \bmod b$  5  
19  $c^{**}(b-1) \bmod b$  7  
5  $a^{**}(c-1) \bmod c$  1  
12  $b^{**}(c-1) \bmod c$  1

7 -->

12  $b^{**}(a-1) \bmod a$  1  
17  $c^{**}(a-1) \bmod a$  1  
7  $a^{**}(b-1) \bmod b$  7  
17  $c^{**}(b-1) \bmod b$  5  
7  $a^{**}(c-1) \bmod c$  1  
12  $b^{**}(c-1) \bmod c$  1

11 -->

12  $b^{**}(a-1) \bmod a$  1  
13  $c^{**}(a-1) \bmod a$  1  
11  $a^{**}(b-1) \bmod b$  11  
13  $c^{**}(b-1) \bmod b$  1  
11  $a^{**}(c-1) \bmod c$  1  
12  $b^{**}(c-1) \bmod c$  1

13 -->

12  $b^{**}(a-1) \bmod a$  1  
11  $c^{**}(a-1) \bmod a$  1  
13  $a^{**}(b-1) \bmod b$  1  
11  $c^{**}(b-1) \bmod b$  11  
13  $a^{**}(c-1) \bmod c$  1  
12  $b^{**}(c-1) \bmod c$  1

les non dg

3 -->

12  $b^{**}(a-1) \bmod a$  0

21  $c^{**}(a-1) \bmod a$  0

3  $a^{**}(b-1) \bmod b$  3

21  $c^{**}(b-1) \bmod b$  9

3  $a^{**}(c-1) \bmod c$  9

12  $b^{**}(c-1) \bmod c$  18

9 -->

12  $b^{**}(a-1) \bmod a$  0

15  $c^{**}(a-1) \bmod a$  0

9  $a^{**}(b-1) \bmod b$  9

15  $c^{**}(b-1) \bmod b$  3

9  $a^{**}(c-1) \bmod c$  6

12  $b^{**}(c-1) \bmod c$  9

.....: 28

les dg

5 -->

14  $b^{**}(a-1) \bmod a$  1

23  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  5

23  $c^{**}(b-1) \bmod b$  9

5  $a^{**}(c-1) \bmod c$  1

14  $b^{**}(c-1) \bmod c$  1

11 -->

14  $b^{**}(a-1) \bmod a$  1

17  $c^{**}(a-1) \bmod a$  1

11  $a^{**}(b-1) \bmod b$  11

17  $c^{**}(b-1) \bmod b$  3

11  $a^{**}(c-1) \bmod c$  1

14  $b^{**}(c-1) \bmod c$  1

les non dg

3 -->

14  $b^{**}(a-1) \bmod a$  1

25  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  3

25  $c^{**}(b-1) \bmod b$  11

3  $a^{**}(c-1) \bmod c$  6

14  $b^{**}(c-1) \bmod c$  16

7 -->

14  $b^{**}(a-1) \bmod a$  0

21  $c^{**}(a-1) \bmod a$  0

7  $a^{**}(b-1) \bmod b$  7

21  $c^{**}(b-1) \bmod b$  7

7  $a^{**}(c-1) \bmod c$  7

14  $b^{**}(c-1) \bmod c$  7

9 -->

14  $b^{**}(a-1) \bmod a$  7

19  $c^{**}(a-1) \bmod a$  1

9  $a^{**}(b-1) \bmod b$  9

19  $c^{**}(b-1) \bmod b$  5

9  $a^{**}(c-1) \bmod c$  1

14  $b^{**}(c-1) \bmod c$  1

13 -->

14  $b^{**}(a-1) \bmod a$  1

15  $c^{**}(a-1) \bmod a$  1

```
13 a**(b-1) mod b 13
15 c**(b-1) mod b 1
13 a**(c-1) mod c 4
14 b**(c-1) mod c 1
15 -->
14 b**(a-1) mod a 1
13 c**(a-1) mod a 4
15 a**(b-1) mod b 1
13 c**(b-1) mod b 13
15 a**(c-1) mod c 1
14 b**(c-1) mod c 1
```

.....: 30

les dg

```
7 -->
15 b**(a-1) mod a 1
23 c**(a-1) mod a 1
7 a**(b-1) mod b 4
23 c**(b-1) mod b 4
7 a**(c-1) mod c 1
15 b**(c-1) mod c 1
11 -->
15 b**(a-1) mod a 1
19 c**(a-1) mod a 1
11 a**(b-1) mod b 1
19 c**(b-1) mod b 1
11 a**(c-1) mod c 1
15 b**(c-1) mod c 1
13 -->
15 b**(a-1) mod a 1
17 c**(a-1) mod a 1
13 a**(b-1) mod b 4
17 c**(b-1) mod b 4
13 a**(c-1) mod c 1
15 b**(c-1) mod c 1
```

les non dg

```
3 -->
15 b**(a-1) mod a 0
27 c**(a-1) mod a 0
3 a**(b-1) mod b 9
27 c**(b-1) mod b 9
3 a**(c-1) mod c 0
15 b**(c-1) mod c 0
5 -->
15 b**(a-1) mod a 0
25 c**(a-1) mod a 0
5 a**(b-1) mod b 10
25 c**(b-1) mod b 10
5 a**(c-1) mod c 0
15 b**(c-1) mod c 0
9 -->
15 b**(a-1) mod a 0
21 c**(a-1) mod a 0
9 a**(b-1) mod b 6
21 c**(b-1) mod b 6
9 a**(c-1) mod c 18
15 b**(c-1) mod c 15
```



```

15 -->
15 b**(a-1) mod a 0
15 c**(a-1) mod a 0
15 a**(b-1) mod b 0
15 c**(b-1) mod b 0
15 a**(c-1) mod c 0
15 b**(c-1) mod c 0

::: 32
les dg
3 -->
16 b**(a-1) mod a 1
29 c**(a-1) mod a 1
3 a**(b-1) mod b 11
29 c**(b-1) mod b 5
3 a**(c-1) mod c 1
16 b**(c-1) mod c 1
13 -->
16 b**(a-1) mod a 1
19 c**(a-1) mod a 1
13 a**(b-1) mod b 5
19 c**(b-1) mod b 11
13 a**(c-1) mod c 1
16 b**(c-1) mod c 1
les non dg
5 -->
16 b**(a-1) mod a 1
27 c**(a-1) mod a 1
5 a**(b-1) mod b 13
27 c**(b-1) mod b 3
5 a**(c-1) mod c 16
16 b**(c-1) mod c 22
7 -->
16 b**(a-1) mod a 1
25 c**(a-1) mod a 1
7 a**(b-1) mod b 7
25 c**(b-1) mod b 9
7 a**(c-1) mod c 1
16 b**(c-1) mod c 11
9 -->
16 b**(a-1) mod a 4
23 c**(a-1) mod a 7
9 a**(b-1) mod b 9
23 c**(b-1) mod b 7
9 a**(c-1) mod c 1
16 b**(c-1) mod c 1
11 -->
16 b**(a-1) mod a 1
21 c**(a-1) mod a 1
11 a**(b-1) mod b 3
21 c**(b-1) mod b 13
11 a**(c-1) mod c 16
16 b**(c-1) mod c 4
15 -->
16 b**(a-1) mod a 1
17 c**(a-1) mod a 4
15 a**(b-1) mod b 15
17 c**(b-1) mod b 1
15 a**(c-1) mod c 1
16 b**(c-1) mod c 1

```

.....: 36

les dg

5 -->

18  $b^{**}(a-1) \bmod a$  1

31  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  11

31  $c^{**}(b-1) \bmod b$  7

5  $a^{**}(c-1) \bmod c$  1

18  $b^{**}(c-1) \bmod c$  1

7 -->

18  $b^{**}(a-1) \bmod a$  1

29  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  13

29  $c^{**}(b-1) \bmod b$  5

7  $a^{**}(c-1) \bmod c$  1

18  $b^{**}(c-1) \bmod c$  1

13 -->

18  $b^{**}(a-1) \bmod a$  1

23  $c^{**}(a-1) \bmod a$  1

13  $a^{**}(b-1) \bmod b$  7

23  $c^{**}(b-1) \bmod b$  11

13  $a^{**}(c-1) \bmod c$  1

18  $b^{**}(c-1) \bmod c$  1

17 -->

18  $b^{**}(a-1) \bmod a$  1

19  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  17

19  $c^{**}(b-1) \bmod b$  1

17  $a^{**}(c-1) \bmod c$  1

18  $b^{**}(c-1) \bmod c$  1

19 -->

18  $b^{**}(a-1) \bmod a$  1

17  $c^{**}(a-1) \bmod a$  1

19  $a^{**}(b-1) \bmod b$  1

17  $c^{**}(b-1) \bmod b$  17

19  $a^{**}(c-1) \bmod c$  1

18  $b^{**}(c-1) \bmod c$  1

les non dg

3 -->

18  $b^{**}(a-1) \bmod a$  0

33  $c^{**}(a-1) \bmod a$  0

3  $a^{**}(b-1) \bmod b$  9

33  $c^{**}(b-1) \bmod b$  9

3  $a^{**}(c-1) \bmod c$  9

18  $b^{**}(c-1) \bmod c$  27

9 -->

18  $b^{**}(a-1) \bmod a$  0

27  $c^{**}(a-1) \bmod a$  0

9  $a^{**}(b-1) \bmod b$  9

27  $c^{**}(b-1) \bmod b$  9

9  $a^{**}(c-1) \bmod c$  0

18  $b^{**}(c-1) \bmod c$  0

```

11 -->
18 b**(a-1) mod a 1
25 c**(a-1) mod a 1
11 a**(b-1) mod b 5
25 c**(b-1) mod b 13
11 a**(c-1) mod c 16
18 b**(c-1) mod c 1
15 -->
18 b**(a-1) mod a 9
21 c**(a-1) mod a 6
15 a**(b-1) mod b 9
21 c**(b-1) mod b 9
15 a**(c-1) mod c 15
18 b**(c-1) mod c 9

::: 40
les dg
3 -->
20 b**(a-1) mod a 1
37 c**(a-1) mod a 1
3 a**(b-1) mod b 7
37 c**(b-1) mod b 13
3 a**(c-1) mod c 1
20 b**(c-1) mod c 1
11 -->
20 b**(a-1) mod a 1
29 c**(a-1) mod a 1
11 a**(b-1) mod b 11
29 c**(b-1) mod b 9
11 a**(c-1) mod c 1
20 b**(c-1) mod c 1
17 -->
20 b**(a-1) mod a 1
23 c**(a-1) mod a 1
17 a**(b-1) mod b 13
23 c**(b-1) mod b 7
17 a**(c-1) mod c 1
20 b**(c-1) mod c 1

les non dg
5 -->
20 b**(a-1) mod a 0
35 c**(a-1) mod a 0
5 a**(b-1) mod b 5
35 c**(b-1) mod b 15
5 a**(c-1) mod c 30
20 b**(c-1) mod c 15
7 -->
20 b**(a-1) mod a 1
33 c**(a-1) mod a 1
7 a**(b-1) mod b 3
33 c**(b-1) mod b 17
7 a**(c-1) mod c 16
20 b**(c-1) mod c 4

```

```

9 -->
20 b**(a-1) mod a 4
31 c**(a-1) mod a 7
9 a**(b-1) mod b 9
31 c**(b-1) mod b 11
9 a**(c-1) mod c 1
20 b**(c-1) mod c 1
13 -->
20 b**(a-1) mod a 1
27 c**(a-1) mod a 1
13 a**(b-1) mod b 17
27 c**(b-1) mod b 3
13 a**(c-1) mod c 25
20 b**(c-1) mod c 4
15 -->
20 b**(a-1) mod a 10
25 c**(a-1) mod a 10
15 a**(b-1) mod b 15
25 c**(b-1) mod b 5
15 a**(c-1) mod c 0
20 b**(c-1) mod c 0
19 -->
20 b**(a-1) mod a 1
21 c**(a-1) mod a 1
19 a**(b-1) mod b 19
21 c**(b-1) mod b 1
19 a**(c-1) mod c 4
20 b**(c-1) mod c 1
21 -->
20 b**(a-1) mod a 1
19 c**(a-1) mod a 4
21 a**(b-1) mod b 1
19 c**(b-1) mod b 19
21 a**(c-1) mod c 1
20 b**(c-1) mod c 1

```

.....: 42

les dg

```

5 -->
21 b**(a-1) mod a 1
37 c**(a-1) mod a 1
5 a**(b-1) mod b 4
37 c**(b-1) mod b 4
5 a**(c-1) mod c 1
21 b**(c-1) mod c 1
11 -->
21 b**(a-1) mod a 1
31 c**(a-1) mod a 1
11 a**(b-1) mod b 16
31 c**(b-1) mod b 16
11 a**(c-1) mod c 1
21 b**(c-1) mod c 1

```

```

13 -->
21 b**(a-1) mod a 1
29 c**(a-1) mod a 1
13 a**(b-1) mod b 1
29 c**(b-1) mod b 1
13 a**(c-1) mod c 1
21 b**(c-1) mod c 1
19 -->
21 b**(a-1) mod a 1
23 c**(a-1) mod a 1
19 a**(b-1) mod b 4
23 c**(b-1) mod b 4
19 a**(c-1) mod c 1
21 b**(c-1) mod c 1

```

les non dg

```

3 -->
21 b**(a-1) mod a 0
39 c**(a-1) mod a 0
3 a**(b-1) mod b 9
39 c**(b-1) mod b 9
3 a**(c-1) mod c 9
21 b**(c-1) mod c 12
7 -->
21 b**(a-1) mod a 0
35 c**(a-1) mod a 0
7 a**(b-1) mod b 7
35 c**(b-1) mod b 7
7 a**(c-1) mod c 14
21 b**(c-1) mod c 21
9 -->
21 b**(a-1) mod a 0
33 c**(a-1) mod a 0
9 a**(b-1) mod b 18
33 c**(b-1) mod b 18
9 a**(c-1) mod c 15
21 b**(c-1) mod c 12
15 -->
21 b**(a-1) mod a 6
27 c**(a-1) mod a 9
15 a**(b-1) mod b 15
27 c**(b-1) mod b 15
15 a**(c-1) mod c 0
21 b**(c-1) mod c 0
17 -->
21 b**(a-1) mod a 1
25 c**(a-1) mod a 1
17 a**(b-1) mod b 16
25 c**(b-1) mod b 16
17 a**(c-1) mod c 21
21 b**(c-1) mod c 6
21 -->
21 b**(a-1) mod a 0
21 c**(a-1) mod a 0
21 a**(b-1) mod b 0
21 c**(b-1) mod b 0
21 a**(c-1) mod c 0
21 b**(c-1) mod c 0

```

..... 44

les dg

3 -->

22  $b^{**}(a-1) \bmod a$  1

41  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  3

41  $c^{**}(b-1) \bmod b$  19

3  $a^{**}(c-1) \bmod c$  1

22  $b^{**}(c-1) \bmod c$  1

7 -->

22  $b^{**}(a-1) \bmod a$  1

37  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  7

37  $c^{**}(b-1) \bmod b$  15

7  $a^{**}(c-1) \bmod c$  1

22  $b^{**}(c-1) \bmod c$  1

13 -->

22  $b^{**}(a-1) \bmod a$  1

31  $c^{**}(a-1) \bmod a$  1

13  $a^{**}(b-1) \bmod b$  13

31  $c^{**}(b-1) \bmod b$  9

13  $a^{**}(c-1) \bmod c$  1

22  $b^{**}(c-1) \bmod c$  1

les non dg

5 -->

22  $b^{**}(a-1) \bmod a$  1

39  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  5

39  $c^{**}(b-1) \bmod b$  17

5  $a^{**}(c-1) \bmod c$  25

22  $b^{**}(c-1) \bmod c$  16

9 -->

22  $b^{**}(a-1) \bmod a$  7

35  $c^{**}(a-1) \bmod a$  1

9  $a^{**}(b-1) \bmod b$  9

35  $c^{**}(b-1) \bmod b$  13

9  $a^{**}(c-1) \bmod c$  16

22  $b^{**}(c-1) \bmod c$  29

11 -->

22  $b^{**}(a-1) \bmod a$  0

33  $c^{**}(a-1) \bmod a$  0

11  $a^{**}(b-1) \bmod b$  11

33  $c^{**}(b-1) \bmod b$  11

11  $a^{**}(c-1) \bmod c$  22

22  $b^{**}(c-1) \bmod c$  22

```
15 -->
22 b**(a-1) mod a 4
29 c**(a-1) mod a 1
15 a**(b-1) mod b 15
29 c**(b-1) mod b 7
15 a**(c-1) mod c 1
22 b**(c-1) mod c 1
17 -->
22 b**(a-1) mod a 1
27 c**(a-1) mod a 1
17 a**(b-1) mod b 17
27 c**(b-1) mod b 5
17 a**(c-1) mod c 19
22 b**(c-1) mod c 16
19 -->
22 b**(a-1) mod a 1
25 c**(a-1) mod a 1
19 a**(b-1) mod b 19
25 c**(b-1) mod b 3
19 a**(c-1) mod c 21
22 b**(c-1) mod c 6
21 -->
22 b**(a-1) mod a 1
23 c**(a-1) mod a 4
21 a**(b-1) mod b 21
23 c**(b-1) mod b 1
21 a**(c-1) mod c 1
22 b**(c-1) mod c 1
23 -->
22 b**(a-1) mod a 1
21 c**(a-1) mod a 1
23 a**(b-1) mod b 1
21 c**(b-1) mod b 21
23 a**(c-1) mod c 4
22 b**(c-1) mod c 1
```

.....: 48

les dg

5 -->

24  $b^{**}(a-1) \bmod a$  1

43  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  5

43  $c^{**}(b-1) \bmod b$  19

5  $a^{**}(c-1) \bmod c$  1

24  $b^{**}(c-1) \bmod c$  1

7 -->

24  $b^{**}(a-1) \bmod a$  1

41  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  7

41  $c^{**}(b-1) \bmod b$  17

7  $a^{**}(c-1) \bmod c$  1

24  $b^{**}(c-1) \bmod c$  1

11 -->

24  $b^{**}(a-1) \bmod a$  1

37  $c^{**}(a-1) \bmod a$  1

11  $a^{**}(b-1) \bmod b$  11

37  $c^{**}(b-1) \bmod b$  13

11  $a^{**}(c-1) \bmod c$  1

24  $b^{**}(c-1) \bmod c$  1

17 -->

24  $b^{**}(a-1) \bmod a$  1

31  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  17

31  $c^{**}(b-1) \bmod b$  7

17  $a^{**}(c-1) \bmod c$  1

24  $b^{**}(c-1) \bmod c$  1

19 -->

24  $b^{**}(a-1) \bmod a$  1

29  $c^{**}(a-1) \bmod a$  1

19  $a^{**}(b-1) \bmod b$  19

29  $c^{**}(b-1) \bmod b$  5

19  $a^{**}(c-1) \bmod c$  1

24  $b^{**}(c-1) \bmod c$  1

les non dg

3 -->

24  $b^{**}(a-1) \bmod a$  0

45  $c^{**}(a-1) \bmod a$  0

3  $a^{**}(b-1) \bmod b$  3

45  $c^{**}(b-1) \bmod b$  21

3  $a^{**}(c-1) \bmod c$  36

24  $b^{**}(c-1) \bmod c$  36

9 -->

24  $b^{**}(a-1) \bmod a$  0

39  $c^{**}(a-1) \bmod a$  0

9  $a^{**}(b-1) \bmod b$  9

39  $c^{**}(b-1) \bmod b$  15

9  $a^{**}(c-1) \bmod c$  3

24  $b^{**}(c-1) \bmod c$  30



```

13 -->
24 b**(a-1) mod a 1
35 c**(a-1) mod a 1
13 a**(b-1) mod b 13
35 c**(b-1) mod b 11
13 a**(c-1) mod c 29
24 b**(c-1) mod c 11
15 -->
24 b**(a-1) mod a 6
33 c**(a-1) mod a 9
15 a**(b-1) mod b 15
33 c**(b-1) mod b 9
15 a**(c-1) mod c 27
24 b**(c-1) mod c 15
21 -->
24 b**(a-1) mod a 9
27 c**(a-1) mod a 15
21 a**(b-1) mod b 21
27 c**(b-1) mod b 3
21 a**(c-1) mod c 0
24 b**(c-1) mod c 0
23 -->
24 b**(a-1) mod a 1
25 c**(a-1) mod a 1
23 a**(b-1) mod b 23
25 c**(b-1) mod b 1
23 a**(c-1) mod c 16
24 b**(c-1) mod c 1
25 -->
24 b**(a-1) mod a 1
23 c**(a-1) mod a 16
25 a**(b-1) mod b 1
23 c**(b-1) mod b 23
25 a**(c-1) mod c 1
24 b**(c-1) mod c 1

```

.....: 50

les dg

```

3 -->
25 b**(a-1) mod a 1
47 c**(a-1) mod a 1
3 a**(b-1) mod b 6
47 c**(b-1) mod b 6
3 a**(c-1) mod c 1
25 b**(c-1) mod c 1
7 -->
25 b**(a-1) mod a 1
43 c**(a-1) mod a 1
7 a**(b-1) mod b 1
43 c**(b-1) mod b 1
7 a**(c-1) mod c 1
25 b**(c-1) mod c 1

```

```
13 -->
25 b**(a-1) mod a 1
37 c**(a-1) mod a 1
13 a**(b-1) mod b 11
37 c**(b-1) mod b 11
13 a**(c-1) mod c 1
25 b**(c-1) mod c 1
19 -->
25 b**(a-1) mod a 1
31 c**(a-1) mod a 1
19 a**(b-1) mod b 21
31 c**(b-1) mod b 21
19 a**(c-1) mod c 1
25 b**(c-1) mod c 1
```

les non dg

```
5 -->
25 b**(a-1) mod a 0
45 c**(a-1) mod a 0
5 a**(b-1) mod b 0
45 c**(b-1) mod b 0
5 a**(c-1) mod c 25
25 b**(c-1) mod c 40
9 -->
25 b**(a-1) mod a 4
41 c**(a-1) mod a 7
9 a**(b-1) mod b 11
41 c**(b-1) mod b 11
9 a**(c-1) mod c 1
25 b**(c-1) mod c 1
11 -->
25 b**(a-1) mod a 1
39 c**(a-1) mod a 1
11 a**(b-1) mod b 16
39 c**(b-1) mod b 16
11 a**(c-1) mod c 4
25 b**(c-1) mod c 1
15 -->
25 b**(a-1) mod a 10
35 c**(a-1) mod a 10
15 a**(b-1) mod b 0
35 c**(b-1) mod b 0
15 a**(c-1) mod c 15
25 b**(c-1) mod c 25
```

```

17 -->
25 b**(a-1) mod a 1
33 c**(a-1) mod a 1
17 a**(b-1) mod b 21
33 c**(b-1) mod b 21
17 a**(c-1) mod c 25
25 b**(c-1) mod c 31
21 -->
25 b**(a-1) mod a 16
29 c**(a-1) mod a 1
21 a**(b-1) mod b 6
29 c**(b-1) mod b 6
21 a**(c-1) mod c 1
25 b**(c-1) mod c 1
23 -->
25 b**(a-1) mod a 1
27 c**(a-1) mod a 1
23 a**(b-1) mod b 16
27 c**(b-1) mod b 16
23 a**(c-1) mod c 7
25 b**(c-1) mod c 13
25 -->
25 b**(a-1) mod a 0
25 c**(a-1) mod a 0
25 a**(b-1) mod b 0
25 c**(b-1) mod b 0
25 a**(c-1) mod c 0
25 b**(c-1) mod c 0

```

..... 52

les dg

```

5 -->
26 b**(a-1) mod a 1
47 c**(a-1) mod a 1
5 a**(b-1) mod b 5
47 c**(b-1) mod b 21
5 a**(c-1) mod c 1
26 b**(c-1) mod c 1
11 -->
26 b**(a-1) mod a 1
41 c**(a-1) mod a 1
11 a**(b-1) mod b 11
41 c**(b-1) mod b 15
11 a**(c-1) mod c 1
26 b**(c-1) mod c 1
23 -->
26 b**(a-1) mod a 1
29 c**(a-1) mod a 1
23 a**(b-1) mod b 23
29 c**(b-1) mod b 3
23 a**(c-1) mod c 1
26 b**(c-1) mod c 1

```

les non dg

3 -->

26  $b^{**}(a-1) \bmod a$  1

49  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  3

49  $c^{**}(b-1) \bmod b$  23

3  $a^{**}(c-1) \bmod c$  43

26  $b^{**}(c-1) \bmod c$  29

7 -->

26  $b^{**}(a-1) \bmod a$  1

45  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  7

45  $c^{**}(b-1) \bmod b$  19

7  $a^{**}(c-1) \bmod c$  31

26  $b^{**}(c-1) \bmod c$  1

9 -->

26  $b^{**}(a-1) \bmod a$  1

43  $c^{**}(a-1) \bmod a$  4

9  $a^{**}(b-1) \bmod b$  9

43  $c^{**}(b-1) \bmod b$  17

9  $a^{**}(c-1) \bmod c$  1

26  $b^{**}(c-1) \bmod c$  1

13 -->

26  $b^{**}(a-1) \bmod a$  0

39  $c^{**}(a-1) \bmod a$  0

13  $a^{**}(b-1) \bmod b$  13

39  $c^{**}(b-1) \bmod b$  13

13  $a^{**}(c-1) \bmod c$  13

26  $b^{**}(c-1) \bmod c$  13

15 -->

26  $b^{**}(a-1) \bmod a$  1

37  $c^{**}(a-1) \bmod a$  4

15  $a^{**}(b-1) \bmod b$  15

37  $c^{**}(b-1) \bmod b$  11

15  $a^{**}(c-1) \bmod c$  1

26  $b^{**}(c-1) \bmod c$  1

17 -->

26  $b^{**}(a-1) \bmod a$  1

35  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  17

35  $c^{**}(b-1) \bmod b$  9

17  $a^{**}(c-1) \bmod c$  4

26  $b^{**}(c-1) \bmod c$  16

19 -->

26  $b^{**}(a-1) \bmod a$  1

33  $c^{**}(a-1) \bmod a$  1

19  $a^{**}(b-1) \bmod b$  19

33  $c^{**}(b-1) \bmod b$  7

19  $a^{**}(c-1) \bmod c$  31

26  $b^{**}(c-1) \bmod c$  16

```

21 -->
26 b**(a-1) mod a 4
31 c**(a-1) mod a 16
21 a**(b-1) mod b 21
31 c**(b-1) mod b 5
21 a**(c-1) mod c 1
26 b**(c-1) mod c 1
25 -->
26 b**(a-1) mod a 1
27 c**(a-1) mod a 16
25 a**(b-1) mod b 25
27 c**(b-1) mod b 1
25 a**(c-1) mod c 13
26 b**(c-1) mod c 1
27 -->
26 b**(a-1) mod a 1
25 c**(a-1) mod a 13
27 a**(b-1) mod b 1
25 c**(b-1) mod b 25
27 a**(c-1) mod c 16
26 b**(c-1) mod c 1

```

.....: 54

les dg

```

7 -->
27 b**(a-1) mod a 1
47 c**(a-1) mod a 1
7 a**(b-1) mod b 4
47 c**(b-1) mod b 4
7 a**(c-1) mod c 1
27 b**(c-1) mod c 1
11 -->
27 b**(a-1) mod a 1
43 c**(a-1) mod a 1
11 a**(b-1) mod b 22
43 c**(b-1) mod b 22
11 a**(c-1) mod c 1
27 b**(c-1) mod c 1
13 -->
27 b**(a-1) mod a 1
41 c**(a-1) mod a 1
13 a**(b-1) mod b 25
41 c**(b-1) mod b 25
13 a**(c-1) mod c 1
27 b**(c-1) mod c 1
17 -->
27 b**(a-1) mod a 1
37 c**(a-1) mod a 1
17 a**(b-1) mod b 19
37 c**(b-1) mod b 19
17 a**(c-1) mod c 1
27 b**(c-1) mod c 1
23 -->
27 b**(a-1) mod a 1
31 c**(a-1) mod a 1
23 a**(b-1) mod b 7
31 c**(b-1) mod b 7
23 a**(c-1) mod c 1
27 b**(c-1) mod c 1

```

les non dg

3 -->

27  $b^{**}(a-1) \bmod a$  0

51  $c^{**}(a-1) \bmod a$  0

3  $a^{**}(b-1) \bmod b$  0

51  $c^{**}(b-1) \bmod b$  0

3  $a^{**}(c-1) \bmod c$  9

27  $b^{**}(c-1) \bmod c$  15

5 -->

27  $b^{**}(a-1) \bmod a$  1

49  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  16

49  $c^{**}(b-1) \bmod b$  16

5  $a^{**}(c-1) \bmod c$  43

27  $b^{**}(c-1) \bmod c$  29

9 -->

27  $b^{**}(a-1) \bmod a$  0

45  $c^{**}(a-1) \bmod a$  0

9  $a^{**}(b-1) \bmod b$  0

45  $c^{**}(b-1) \bmod b$  0

9  $a^{**}(c-1) \bmod c$  36

27  $b^{**}(c-1) \bmod c$  36

15 -->

27  $b^{**}(a-1) \bmod a$  9

39  $c^{**}(a-1) \bmod a$  6

15  $a^{**}(b-1) \bmod b$  0

39  $c^{**}(b-1) \bmod b$  0

15  $a^{**}(c-1) \bmod c$  30

27  $b^{**}(c-1) \bmod c$  27

19 -->

27  $b^{**}(a-1) \bmod a$  1

35  $c^{**}(a-1) \bmod a$  1

19  $a^{**}(b-1) \bmod b$  10

35  $c^{**}(b-1) \bmod b$  10

19  $a^{**}(c-1) \bmod c$  16

27  $b^{**}(c-1) \bmod c$  29

21 -->

27  $b^{**}(a-1) \bmod a$  15

33  $c^{**}(a-1) \bmod a$  18

21  $a^{**}(b-1) \bmod b$  0

33  $c^{**}(b-1) \bmod b$  0

21  $a^{**}(c-1) \bmod c$  12

27  $b^{**}(c-1) \bmod c$  3

25 -->

27  $b^{**}(a-1) \bmod a$  16

29  $c^{**}(a-1) \bmod a$  6

25  $a^{**}(b-1) \bmod b$  13

29  $c^{**}(b-1) \bmod b$  13

25  $a^{**}(c-1) \bmod c$  1

27  $b^{**}(c-1) \bmod c$  1

```

27 -->
27 b**(a-1) mod a 0
27 c**(a-1) mod a 0
27 a**(b-1) mod b 0
27 c**(b-1) mod b 0
27 a**(c-1) mod c 0
27 b**(c-1) mod c 0

::: 56
les dg
3 -->
28 b**(a-1) mod a 1
53 c**(a-1) mod a 1
3 a**(b-1) mod b 27
53 c**(b-1) mod b 1
3 a**(c-1) mod c 1
28 b**(c-1) mod c 1
13 -->
28 b**(a-1) mod a 1
43 c**(a-1) mod a 1
13 a**(b-1) mod b 13
43 c**(b-1) mod b 15
13 a**(c-1) mod c 1
28 b**(c-1) mod c 1
19 -->
28 b**(a-1) mod a 1
37 c**(a-1) mod a 1
19 a**(b-1) mod b 27
37 c**(b-1) mod b 1
19 a**(c-1) mod c 1
28 b**(c-1) mod c 1

les non dg
5 -->
28 b**(a-1) mod a 1
51 c**(a-1) mod a 1
5 a**(b-1) mod b 13
51 c**(b-1) mod b 15
5 a**(c-1) mod c 25
28 b**(c-1) mod c 19
7 -->
28 b**(a-1) mod a 0
49 c**(a-1) mod a 0
7 a**(b-1) mod b 7
49 c**(b-1) mod b 21
7 a**(c-1) mod c 0
28 b**(c-1) mod c 0
9 -->
28 b**(a-1) mod a 1
47 c**(a-1) mod a 4
9 a**(b-1) mod b 1
47 c**(b-1) mod b 27
9 a**(c-1) mod c 1
28 b**(c-1) mod c 1

```

```

11 -->
28 b**(a-1) mod a 1
45 c**(a-1) mod a 1
11 a**(b-1) mod b 15
45 c**(b-1) mod b 13
11 a**(c-1) mod c 31
28 b**(c-1) mod c 1
15 -->
28 b**(a-1) mod a 4
41 c**(a-1) mod a 1
15 a**(b-1) mod b 15
41 c**(b-1) mod b 13
15 a**(c-1) mod c 1
28 b**(c-1) mod c 1
17 -->
28 b**(a-1) mod a 1
39 c**(a-1) mod a 1
17 a**(b-1) mod b 13
39 c**(b-1) mod b 15
17 a**(c-1) mod c 16
28 b**(c-1) mod c 4
21 -->
28 b**(a-1) mod a 7
35 c**(a-1) mod a 7
21 a**(b-1) mod b 21
35 c**(b-1) mod b 7
21 a**(c-1) mod c 21
28 b**(c-1) mod c 14
23 -->
28 b**(a-1) mod a 1
33 c**(a-1) mod a 1
23 a**(b-1) mod b 15
33 c**(b-1) mod b 13
23 a**(c-1) mod c 1
28 b**(c-1) mod c 25
25 -->
28 b**(a-1) mod a 6
31 c**(a-1) mod a 21
25 a**(b-1) mod b 1
31 c**(b-1) mod b 27
25 a**(c-1) mod c 1
28 b**(c-1) mod c 1
27 -->
28 b**(a-1) mod a 1
29 c**(a-1) mod a 13
27 a**(b-1) mod b 27
29 c**(b-1) mod b 1
27 a**(c-1) mod c 1
28 b**(c-1) mod c 1
29 -->
28 b**(a-1) mod a 1
27 c**(a-1) mod a 1
29 a**(b-1) mod b 1
27 c**(b-1) mod b 27
29 a**(c-1) mod c 13
28 b**(c-1) mod c 1

```



```

:~:~:~:~:~:~:~: 60
les dg
7 -->
30 b**(a-1) mod a 1
53 c**(a-1) mod a 1
7 a**(b-1) mod b 7
53 c**(b-1) mod b 23
7 a**(c-1) mod c 1
30 b**(c-1) mod c 1
13 -->
30 b**(a-1) mod a 1
47 c**(a-1) mod a 1
13 a**(b-1) mod b 13
47 c**(b-1) mod b 17
13 a**(c-1) mod c 1
30 b**(c-1) mod c 1
17 -->
30 b**(a-1) mod a 1
43 c**(a-1) mod a 1
17 a**(b-1) mod b 17
43 c**(b-1) mod b 13
17 a**(c-1) mod c 1
30 b**(c-1) mod c 1
19 -->
30 b**(a-1) mod a 1
41 c**(a-1) mod a 1
19 a**(b-1) mod b 19
41 c**(b-1) mod b 11
19 a**(c-1) mod c 1
30 b**(c-1) mod c 1
23 -->
30 b**(a-1) mod a 1
37 c**(a-1) mod a 1
23 a**(b-1) mod b 23
37 c**(b-1) mod b 7
23 a**(c-1) mod c 1
30 b**(c-1) mod c 1
29 -->
30 b**(a-1) mod a 1
31 c**(a-1) mod a 1
29 a**(b-1) mod b 29
31 c**(b-1) mod b 1
29 a**(c-1) mod c 1
30 b**(c-1) mod c 1
31 -->
30 b**(a-1) mod a 1
29 c**(a-1) mod a 1
31 a**(b-1) mod b 1
29 c**(b-1) mod b 29
31 a**(c-1) mod c 1
30 b**(c-1) mod c 1

```

les non dg

3 -->

30  $b^{**}(a-1) \bmod a$  0

57  $c^{**}(a-1) \bmod a$  0

3  $a^{**}(b-1) \bmod b$  3

57  $c^{**}(b-1) \bmod b$  27

3  $a^{**}(c-1) \bmod c$  9

30  $b^{**}(c-1) \bmod c$  45

5 -->

30  $b^{**}(a-1) \bmod a$  0

55  $c^{**}(a-1) \bmod a$  0

5  $a^{**}(b-1) \bmod b$  5

55  $c^{**}(b-1) \bmod b$  25

5  $a^{**}(c-1) \bmod c$  20

30  $b^{**}(c-1) \bmod c$  15

9 -->

30  $b^{**}(a-1) \bmod a$  0

51  $c^{**}(a-1) \bmod a$  0

9  $a^{**}(b-1) \bmod b$  9

51  $c^{**}(b-1) \bmod b$  21

9  $a^{**}(c-1) \bmod c$  30

30  $b^{**}(c-1) \bmod c$  33

11 -->

30  $b^{**}(a-1) \bmod a$  1

49  $c^{**}(a-1) \bmod a$  1

11  $a^{**}(b-1) \bmod b$  11

49  $c^{**}(b-1) \bmod b$  19

11  $a^{**}(c-1) \bmod c$  15

30  $b^{**}(c-1) \bmod c$  1

15 -->

30  $b^{**}(a-1) \bmod a$  0

45  $c^{**}(a-1) \bmod a$  0

15  $a^{**}(b-1) \bmod b$  15

45  $c^{**}(b-1) \bmod b$  15

15  $a^{**}(c-1) \bmod c$  0

30  $b^{**}(c-1) \bmod c$  0

21 -->

30  $b^{**}(a-1) \bmod a$  18

39  $c^{**}(a-1) \bmod a$  9

21  $a^{**}(b-1) \bmod b$  21

39  $c^{**}(b-1) \bmod b$  9

21  $a^{**}(c-1) \bmod c$  12

30  $b^{**}(c-1) \bmod c$  3

25 -->

30  $b^{**}(a-1) \bmod a$  0

35  $c^{**}(a-1) \bmod a$  0

25  $a^{**}(b-1) \bmod b$  25

35  $c^{**}(b-1) \bmod b$  5

25  $a^{**}(c-1) \bmod c$  25

30  $b^{**}(c-1) \bmod c$  30

27 -->

30  $b^{**}(a-1) \bmod a$  0

33  $c^{**}(a-1) \bmod a$  0

27  $a^{**}(b-1) \bmod b$  27

33  $c^{**}(b-1) \bmod b$  3

27  $a^{**}(c-1) \bmod c$  3

30  $b^{**}(c-1) \bmod c$  9

.....: 64

les dg

3 -->

32  $b^{**}(a-1) \bmod a$  1

61  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  11

61  $c^{**}(b-1) \bmod b$  21

3  $a^{**}(c-1) \bmod c$  1

32  $b^{**}(c-1) \bmod c$  1

5 -->

32  $b^{**}(a-1) \bmod a$  1

59  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  13

59  $c^{**}(b-1) \bmod b$  19

5  $a^{**}(c-1) \bmod c$  1

32  $b^{**}(c-1) \bmod c$  1

11 -->

32  $b^{**}(a-1) \bmod a$  1

53  $c^{**}(a-1) \bmod a$  1

11  $a^{**}(b-1) \bmod b$  3

53  $c^{**}(b-1) \bmod b$  29

11  $a^{**}(c-1) \bmod c$  1

32  $b^{**}(c-1) \bmod c$  1

17 -->

32  $b^{**}(a-1) \bmod a$  1

47  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  17

47  $c^{**}(b-1) \bmod b$  15

17  $a^{**}(c-1) \bmod c$  1

32  $b^{**}(c-1) \bmod c$  1

23 -->

32  $b^{**}(a-1) \bmod a$  1

41  $c^{**}(a-1) \bmod a$  1

23  $a^{**}(b-1) \bmod b$  7

41  $c^{**}(b-1) \bmod b$  25

23  $a^{**}(c-1) \bmod c$  1

32  $b^{**}(c-1) \bmod c$  1

les non dg

7 -->

32  $b^{**}(a-1) \bmod a$  1

57  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  23

57  $c^{**}(b-1) \bmod b$  9

7  $a^{**}(c-1) \bmod c$  49

32  $b^{**}(c-1) \bmod c$  55

9 -->

32  $b^{**}(a-1) \bmod a$  7

55  $c^{**}(a-1) \bmod a$  1

9  $a^{**}(b-1) \bmod b$  25

55  $c^{**}(b-1) \bmod b$  7

9  $a^{**}(c-1) \bmod c$  16

32  $b^{**}(c-1) \bmod c$  34

```

13 -->
32 b**(a-1) mod a 1
51 c**(a-1) mod a 1
13 a**(b-1) mod b 5
51 c**(b-1) mod b 27
13 a**(c-1) mod c 16
32 b**(c-1) mod c 4
15 -->
32 b**(a-1) mod a 4
49 c**(a-1) mod a 1
15 a**(b-1) mod b 15
49 c**(b-1) mod b 17
15 a**(c-1) mod c 36
32 b**(c-1) mod c 22
19 -->
32 b**(a-1) mod a 1
45 c**(a-1) mod a 1
19 a**(b-1) mod b 27
45 c**(b-1) mod b 5
19 a**(c-1) mod c 1
32 b**(c-1) mod c 16
21 -->
32 b**(a-1) mod a 16
43 c**(a-1) mod a 1
21 a**(b-1) mod b 29
43 c**(b-1) mod b 3
21 a**(c-1) mod c 1
32 b**(c-1) mod c 1
25 -->
32 b**(a-1) mod a 1
39 c**(a-1) mod a 16
25 a**(b-1) mod b 9
39 c**(b-1) mod b 23
25 a**(c-1) mod c 1
32 b**(c-1) mod c 10
27 -->
32 b**(a-1) mod a 16
37 c**(a-1) mod a 19
27 a**(b-1) mod b 19
37 c**(b-1) mod b 13
27 a**(c-1) mod c 1
32 b**(c-1) mod c 1
29 -->
32 b**(a-1) mod a 1
35 c**(a-1) mod a 1
29 a**(b-1) mod b 21
35 c**(b-1) mod b 11
29 a**(c-1) mod c 1
32 b**(c-1) mod c 4
31 -->
32 b**(a-1) mod a 1
33 c**(a-1) mod a 1
31 a**(b-1) mod b 31
33 c**(b-1) mod b 1
31 a**(c-1) mod c 4
32 b**(c-1) mod c 1

```

```

33 -->
32 b**(a-1) mod a 1
31 c**(a-1) mod a 4
33 a**(b-1) mod b 1
31 c**(b-1) mod b 31
33 a**(c-1) mod c 1
32 b**(c-1) mod c 1

::: 66
les dg
5 -->
33 b**(a-1) mod a 1
61 c**(a-1) mod a 1
5 a**(b-1) mod b 25
61 c**(b-1) mod b 25
5 a**(c-1) mod c 1
33 b**(c-1) mod c 1
7 -->
33 b**(a-1) mod a 1
59 c**(a-1) mod a 1
7 a**(b-1) mod b 16
59 c**(b-1) mod b 16
7 a**(c-1) mod c 1
33 b**(c-1) mod c 1
13 -->
33 b**(a-1) mod a 1
53 c**(a-1) mod a 1
13 a**(b-1) mod b 4
53 c**(b-1) mod b 4
13 a**(c-1) mod c 1
33 b**(c-1) mod c 1
19 -->
33 b**(a-1) mod a 1
47 c**(a-1) mod a 1
19 a**(b-1) mod b 31
47 c**(b-1) mod b 31
19 a**(c-1) mod c 1
33 b**(c-1) mod c 1
23 -->
33 b**(a-1) mod a 1
43 c**(a-1) mod a 1
23 a**(b-1) mod b 1
43 c**(b-1) mod b 1
23 a**(c-1) mod c 1
33 b**(c-1) mod c 1
29 -->
33 b**(a-1) mod a 1
37 c**(a-1) mod a 1
29 a**(b-1) mod b 16
37 c**(b-1) mod b 16
29 a**(c-1) mod c 1
33 b**(c-1) mod c 1

```

les non dg

3 -->

33  $b^{**}(a-1) \bmod a$  0

63  $c^{**}(a-1) \bmod a$  0

3  $a^{**}(b-1) \bmod b$  9

63  $c^{**}(b-1) \bmod b$  9

3  $a^{**}(c-1) \bmod c$  9

33  $b^{**}(c-1) \bmod c$  18

9 -->

33  $b^{**}(a-1) \bmod a$  0

57  $c^{**}(a-1) \bmod a$  0

9  $a^{**}(b-1) \bmod b$  15

57  $c^{**}(b-1) \bmod b$  15

9  $a^{**}(c-1) \bmod c$  24

33  $b^{**}(c-1) \bmod c$  6

11 -->

33  $b^{**}(a-1) \bmod a$  0

55  $c^{**}(a-1) \bmod a$  0

11  $a^{**}(b-1) \bmod b$  22

55  $c^{**}(b-1) \bmod b$  22

11  $a^{**}(c-1) \bmod c$  11

33  $b^{**}(c-1) \bmod c$  44

15 -->

33  $b^{**}(a-1) \bmod a$  9

51  $c^{**}(a-1) \bmod a$  6

15  $a^{**}(b-1) \bmod b$  27

51  $c^{**}(b-1) \bmod b$  27

15  $a^{**}(c-1) \bmod c$  21

33  $b^{**}(c-1) \bmod c$  18

17 -->

33  $b^{**}(a-1) \bmod a$  1

49  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  25

49  $c^{**}(b-1) \bmod b$  25

17  $a^{**}(c-1) \bmod c$  22

33  $b^{**}(c-1) \bmod c$  8

21 -->

33  $b^{**}(a-1) \bmod a$  18

45  $c^{**}(a-1) \bmod a$  9

21  $a^{**}(b-1) \bmod b$  12

45  $c^{**}(b-1) \bmod b$  12

21  $a^{**}(c-1) \bmod c$  36

33  $b^{**}(c-1) \bmod c$  36

25 -->

33  $b^{**}(a-1) \bmod a$  21

41  $c^{**}(a-1) \bmod a$  11

25  $a^{**}(b-1) \bmod b$  31

41  $c^{**}(b-1) \bmod b$  31

25  $a^{**}(c-1) \bmod c$  1

33  $b^{**}(c-1) \bmod c$  1

```

27 -->
33 b**(a-1) mod a 0
39 c**(a-1) mod a 0
27 a**(b-1) mod b 3
39 c**(b-1) mod b 3
27 a**(c-1) mod c 27
33 b**(c-1) mod c 36
31 -->
33 b**(a-1) mod a 1
35 c**(a-1) mod a 1
31 a**(b-1) mod b 4
35 c**(b-1) mod b 4
31 a**(c-1) mod c 11
33 b**(c-1) mod c 9
33 -->
33 b**(a-1) mod a 0
33 c**(a-1) mod a 0
33 a**(b-1) mod b 0
33 c**(b-1) mod b 0
33 a**(c-1) mod c 0
33 b**(c-1) mod c 0

```

.....: 68

les dg

```

7 -->
34 b**(a-1) mod a 1
61 c**(a-1) mod a 1
7 a**(b-1) mod b 7
61 c**(b-1) mod b 27
7 a**(c-1) mod c 1
34 b**(c-1) mod c 1
31 -->
34 b**(a-1) mod a 1
37 c**(a-1) mod a 1
31 a**(b-1) mod b 31
37 c**(b-1) mod b 3
31 a**(c-1) mod c 1
34 b**(c-1) mod c 1

```

les non dg

```

3 -->
34 b**(a-1) mod a 1
65 c**(a-1) mod a 1
3 a**(b-1) mod b 3
65 c**(b-1) mod b 31
3 a**(c-1) mod c 16
34 b**(c-1) mod c 1
5 -->
34 b**(a-1) mod a 1
63 c**(a-1) mod a 1
5 a**(b-1) mod b 5
63 c**(b-1) mod b 29
5 a**(c-1) mod c 25
34 b**(c-1) mod c 22

```

```

9 -->
34 b**(a-1) mod a 4
59 c**(a-1) mod a 7
9 a**(b-1) mod b 9
59 c**(b-1) mod b 25
9 a**(c-1) mod c 1
34 b**(c-1) mod c 1
11 -->
34 b**(a-1) mod a 1
57 c**(a-1) mod a 1
11 a**(b-1) mod b 11
57 c**(b-1) mod b 23
11 a**(c-1) mod c 7
34 b**(c-1) mod c 16
13 -->
34 b**(a-1) mod a 1
55 c**(a-1) mod a 1
13 a**(b-1) mod b 13
55 c**(b-1) mod b 21
13 a**(c-1) mod c 49
34 b**(c-1) mod c 1
15 -->
34 b**(a-1) mod a 1
53 c**(a-1) mod a 4
15 a**(b-1) mod b 15
53 c**(b-1) mod b 19
15 a**(c-1) mod c 1
34 b**(c-1) mod c 1
17 -->
34 b**(a-1) mod a 0
51 c**(a-1) mod a 0
17 a**(b-1) mod b 17
51 c**(b-1) mod b 17
17 a**(c-1) mod c 34
34 b**(c-1) mod c 34
19 -->
34 b**(a-1) mod a 1
49 c**(a-1) mod a 1
19 a**(b-1) mod b 19
49 c**(b-1) mod b 15
19 a**(c-1) mod c 1
34 b**(c-1) mod c 36
21 -->
34 b**(a-1) mod a 1
47 c**(a-1) mod a 4
21 a**(b-1) mod b 21
47 c**(b-1) mod b 13
21 a**(c-1) mod c 1
34 b**(c-1) mod c 1

```



```

23 -->
34 b**(a-1) mod a 1
45 c**(a-1) mod a 1
23 a**(b-1) mod b 23
45 c**(b-1) mod b 11
23 a**(c-1) mod c 16
34 b**(c-1) mod c 31
25 -->
34 b**(a-1) mod a 11
43 c**(a-1) mod a 1
25 a**(b-1) mod b 25
43 c**(b-1) mod b 9
25 a**(c-1) mod c 1
34 b**(c-1) mod c 1
27 -->
34 b**(a-1) mod a 4
41 c**(a-1) mod a 25
27 a**(b-1) mod b 27
41 c**(b-1) mod b 7
27 a**(c-1) mod c 1
34 b**(c-1) mod c 1
29 -->
34 b**(a-1) mod a 1
39 c**(a-1) mod a 1
29 a**(b-1) mod b 29
39 c**(b-1) mod b 5
29 a**(c-1) mod c 22
34 b**(c-1) mod c 25
33 -->
34 b**(a-1) mod a 1
35 c**(a-1) mod a 4
33 a**(b-1) mod b 33
35 c**(b-1) mod b 1
33 a**(c-1) mod c 9
34 b**(c-1) mod c 1
35 -->
34 b**(a-1) mod a 1
33 c**(a-1) mod a 9
35 a**(b-1) mod b 1
33 c**(b-1) mod b 33
35 a**(c-1) mod c 4
34 b**(c-1) mod c 1

```

.....: 70

les dg

3 -->

35  $b^{**}(a-1) \bmod a$  1

67  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  4

67  $c^{**}(b-1) \bmod b$  4

3  $a^{**}(c-1) \bmod c$  1

35  $b^{**}(c-1) \bmod c$  1

11 -->

35  $b^{**}(a-1) \bmod a$  1

59  $c^{**}(a-1) \bmod a$  1

11  $a^{**}(b-1) \bmod b$  11

59  $c^{**}(b-1) \bmod b$  11

11  $a^{**}(c-1) \bmod c$  1

35  $b^{**}(c-1) \bmod c$  1

17 -->

35  $b^{**}(a-1) \bmod a$  1

53  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  4

53  $c^{**}(b-1) \bmod b$  4

17  $a^{**}(c-1) \bmod c$  1

35  $b^{**}(c-1) \bmod c$  1

23 -->

35  $b^{**}(a-1) \bmod a$  1

47  $c^{**}(a-1) \bmod a$  1

23  $a^{**}(b-1) \bmod b$  9

47  $c^{**}(b-1) \bmod b$  9

23  $a^{**}(c-1) \bmod c$  1

35  $b^{**}(c-1) \bmod c$  1

29 -->

35  $b^{**}(a-1) \bmod a$  1

41  $c^{**}(a-1) \bmod a$  1

29  $a^{**}(b-1) \bmod b$  1

41  $c^{**}(b-1) \bmod b$  1

29  $a^{**}(c-1) \bmod c$  1

35  $b^{**}(c-1) \bmod c$  1

les non dg

5 -->

35  $b^{**}(a-1) \bmod a$  0

65  $c^{**}(a-1) \bmod a$  0

5  $a^{**}(b-1) \bmod b$  30

65  $c^{**}(b-1) \bmod b$  30

5  $a^{**}(c-1) \bmod c$  40

35  $b^{**}(c-1) \bmod c$  35

7 -->

35  $b^{**}(a-1) \bmod a$  0

63  $c^{**}(a-1) \bmod a$  0

7  $a^{**}(b-1) \bmod b$  14

63  $c^{**}(b-1) \bmod b$  14

7  $a^{**}(c-1) \bmod c$  49

35  $b^{**}(c-1) \bmod c$  28

```

9 -->
35 b**(a-1) mod a 1
61 c**(a-1) mod a 4
9 a**(b-1) mod b 16
61 c**(b-1) mod b 16
9 a**(c-1) mod c 1
35 b**(c-1) mod c 1
13 -->
35 b**(a-1) mod a 1
57 c**(a-1) mod a 1
13 a**(b-1) mod b 29
57 c**(b-1) mod b 29
13 a**(c-1) mod c 55
35 b**(c-1) mod c 28
15 -->
35 b**(a-1) mod a 10
55 c**(a-1) mod a 10
15 a**(b-1) mod b 15
55 c**(b-1) mod b 15
15 a**(c-1) mod c 25
35 b**(c-1) mod c 5
19 -->
35 b**(a-1) mod a 1
51 c**(a-1) mod a 1
19 a**(b-1) mod b 16
51 c**(b-1) mod b 16
19 a**(c-1) mod c 4
35 b**(c-1) mod c 1
21 -->
35 b**(a-1) mod a 7
49 c**(a-1) mod a 7
21 a**(b-1) mod b 21
49 c**(b-1) mod b 21
21 a**(c-1) mod c 0
35 b**(c-1) mod c 0
25 -->
35 b**(a-1) mod a 0
45 c**(a-1) mod a 0
25 a**(b-1) mod b 25
45 c**(b-1) mod b 25
25 a**(c-1) mod c 40
35 b**(c-1) mod c 10
27 -->
35 b**(a-1) mod a 10
43 c**(a-1) mod a 22
27 a**(b-1) mod b 29
43 c**(b-1) mod b 29
27 a**(c-1) mod c 1
35 b**(c-1) mod c 1
31 -->
35 b**(a-1) mod a 1
39 c**(a-1) mod a 1
31 a**(b-1) mod b 11
39 c**(b-1) mod b 11
31 a**(c-1) mod c 25
35 b**(c-1) mod c 16

```

```

33 -->
35 b**(a-1) mod a 4
37 c**(a-1) mod a 16
33 a**(b-1) mod b 9
37 c**(b-1) mod b 9
33 a**(c-1) mod c 1
35 b**(c-1) mod c 1
35 -->
35 b**(a-1) mod a 0
35 c**(a-1) mod a 0
35 a**(b-1) mod b 0
35 c**(b-1) mod b 0
35 a**(c-1) mod c 0
35 b**(c-1) mod c 0

```

.....: 72

les dg

```

5 -->
36 b**(a-1) mod a 1
67 c**(a-1) mod a 1
5 a**(b-1) mod b 29
67 c**(b-1) mod b 7
5 a**(c-1) mod c 1
36 b**(c-1) mod c 1
11 -->
36 b**(a-1) mod a 1
61 c**(a-1) mod a 1
11 a**(b-1) mod b 23
61 c**(b-1) mod b 13
11 a**(c-1) mod c 1
36 b**(c-1) mod c 1
13 -->
36 b**(a-1) mod a 1
59 c**(a-1) mod a 1
13 a**(b-1) mod b 25
59 c**(b-1) mod b 11
13 a**(c-1) mod c 1
36 b**(c-1) mod c 1
19 -->
36 b**(a-1) mod a 1
53 c**(a-1) mod a 1
19 a**(b-1) mod b 19
53 c**(b-1) mod b 17
19 a**(c-1) mod c 1
36 b**(c-1) mod c 1
29 -->
36 b**(a-1) mod a 1
43 c**(a-1) mod a 1
29 a**(b-1) mod b 5
43 c**(b-1) mod b 31
29 a**(c-1) mod c 1
36 b**(c-1) mod c 1

```

```
31 -->
36 b**(a-1) mod a 1
41 c**(a-1) mod a 1
31 a**(b-1) mod b 7
41 c**(b-1) mod b 29
31 a**(c-1) mod c 1
36 b**(c-1) mod c 1
```

#### les non dg

```
3 -->
36 b**(a-1) mod a 0
69 c**(a-1) mod a 0
3 a**(b-1) mod b 27
69 c**(b-1) mod b 9
3 a**(c-1) mod c 9
36 b**(c-1) mod c 54
7 -->
36 b**(a-1) mod a 1
65 c**(a-1) mod a 1
7 a**(b-1) mod b 31
65 c**(b-1) mod b 5
7 a**(c-1) mod c 61
36 b**(c-1) mod c 16
9 -->
36 b**(a-1) mod a 0
63 c**(a-1) mod a 0
9 a**(b-1) mod b 9
63 c**(b-1) mod b 27
9 a**(c-1) mod c 18
36 b**(c-1) mod c 36
15 -->
36 b**(a-1) mod a 6
57 c**(a-1) mod a 9
15 a**(b-1) mod b 27
57 c**(b-1) mod b 9
15 a**(c-1) mod c 54
36 b**(c-1) mod c 42
17 -->
36 b**(a-1) mod a 1
55 c**(a-1) mod a 1
17 a**(b-1) mod b 17
55 c**(b-1) mod b 19
17 a**(c-1) mod c 9
36 b**(c-1) mod c 26
21 -->
36 b**(a-1) mod a 15
51 c**(a-1) mod a 18
21 a**(b-1) mod b 9
51 c**(b-1) mod b 27
21 a**(c-1) mod c 33
36 b**(c-1) mod c 21
```

```

23 -->
36 b**(a-1) mod a 1
49 c**(a-1) mod a 1
23 a**(b-1) mod b 11
49 c**(b-1) mod b 25
23 a**(c-1) mod c 29
36 b**(c-1) mod c 15
25 -->
36 b**(a-1) mod a 16
47 c**(a-1) mod a 6
25 a**(b-1) mod b 13
47 c**(b-1) mod b 23
25 a**(c-1) mod c 1
36 b**(c-1) mod c 1
27 -->
36 b**(a-1) mod a 0
45 c**(a-1) mod a 0
27 a**(b-1) mod b 27
45 c**(b-1) mod b 9
27 a**(c-1) mod c 36
36 b**(c-1) mod c 36
33 -->
36 b**(a-1) mod a 9
39 c**(a-1) mod a 3
33 a**(b-1) mod b 9
39 c**(b-1) mod b 27
33 a**(c-1) mod c 36
36 b**(c-1) mod c 9
35 -->
36 b**(a-1) mod a 1
37 c**(a-1) mod a 9
35 a**(b-1) mod b 35
37 c**(b-1) mod b 1
35 a**(c-1) mod c 1
36 b**(c-1) mod c 1
37 -->
36 b**(a-1) mod a 1
35 c**(a-1) mod a 1
37 a**(b-1) mod b 1
35 c**(b-1) mod b 35
37 a**(c-1) mod c 9
36 b**(c-1) mod c 1

```

.....: 76

les dg

3 -->

38  $b^{**}(a-1) \bmod a$  1

73  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  3

73  $c^{**}(b-1) \bmod b$  35

3  $a^{**}(c-1) \bmod c$  1

38  $b^{**}(c-1) \bmod c$  1

5 -->

38  $b^{**}(a-1) \bmod a$  1

71  $c^{**}(a-1) \bmod a$  1

5  $a^{**}(b-1) \bmod b$  5

71  $c^{**}(b-1) \bmod b$  33

5  $a^{**}(c-1) \bmod c$  1

38  $b^{**}(c-1) \bmod c$  1

17 -->

38  $b^{**}(a-1) \bmod a$  1

59  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  17

59  $c^{**}(b-1) \bmod b$  21

17  $a^{**}(c-1) \bmod c$  1

38  $b^{**}(c-1) \bmod c$  1

23 -->

38  $b^{**}(a-1) \bmod a$  1

53  $c^{**}(a-1) \bmod a$  1

23  $a^{**}(b-1) \bmod b$  23

53  $c^{**}(b-1) \bmod b$  15

23  $a^{**}(c-1) \bmod c$  1

38  $b^{**}(c-1) \bmod c$  1

29 -->

38  $b^{**}(a-1) \bmod a$  1

47  $c^{**}(a-1) \bmod a$  1

29  $a^{**}(b-1) \bmod b$  29

47  $c^{**}(b-1) \bmod b$  9

29  $a^{**}(c-1) \bmod c$  1

38  $b^{**}(c-1) \bmod c$  1

les non dg

7 -->

38  $b^{**}(a-1) \bmod a$  1

69  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  7

69  $c^{**}(b-1) \bmod b$  31

7  $a^{**}(c-1) \bmod c$  49

38  $b^{**}(c-1) \bmod c$  64

9 -->

38  $b^{**}(a-1) \bmod a$  4

67  $c^{**}(a-1) \bmod a$  7

9  $a^{**}(b-1) \bmod b$  9

67  $c^{**}(b-1) \bmod b$  29

9  $a^{**}(c-1) \bmod c$  1

38  $b^{**}(c-1) \bmod c$  1

```

11 -->
38 b**(a-1) mod a 1
65 c**(a-1) mod a 1
11 a**(b-1) mod b 11
65 c**(b-1) mod b 27
11 a**(c-1) mod c 16
38 b**(c-1) mod c 1
13 -->
38 b**(a-1) mod a 1
63 c**(a-1) mod a 1
13 a**(b-1) mod b 13
63 c**(b-1) mod b 25
13 a**(c-1) mod c 43
38 b**(c-1) mod c 58
15 -->
38 b**(a-1) mod a 4
61 c**(a-1) mod a 1
15 a**(b-1) mod b 15
61 c**(b-1) mod b 23
15 a**(c-1) mod c 1
38 b**(c-1) mod c 1
19 -->
38 b**(a-1) mod a 0
57 c**(a-1) mod a 0
19 a**(b-1) mod b 19
57 c**(b-1) mod b 19
19 a**(c-1) mod c 19
38 b**(c-1) mod c 19
21 -->
38 b**(a-1) mod a 16
55 c**(a-1) mod a 1
21 a**(b-1) mod b 21
55 c**(b-1) mod b 17
21 a**(c-1) mod c 1
38 b**(c-1) mod c 9
23 -->
34 b**(a-1) mod a 1
45 c**(a-1) mod a 1
23 a**(b-1) mod b 23
45 c**(b-1) mod b 11
23 a**(c-1) mod c 16
34 b**(c-1) mod c 31
25 -->
34 b**(a-1) mod a 11
43 c**(a-1) mod a 1
25 a**(b-1) mod b 25
43 c**(b-1) mod b 9
25 a**(c-1) mod c 1
34 b**(c-1) mod c 1
27 -->
34 b**(a-1) mod a 4
41 c**(a-1) mod a 25
27 a**(b-1) mod b 27
41 c**(b-1) mod b 7
27 a**(c-1) mod c 1
34 b**(c-1) mod c 1

```



```

31 -->
38 b**(a-1) mod a 1
45 c**(a-1) mod a 1
31 a**(b-1) mod b 31
45 c**(b-1) mod b 7
31 a**(c-1) mod c 16
38 b**(c-1) mod c 31
33 -->
38 b**(a-1) mod a 25
43 c**(a-1) mod a 1
33 a**(b-1) mod b 33
43 c**(b-1) mod b 5
33 a**(c-1) mod c 1
38 b**(c-1) mod c 1
35 -->
38 b**(a-1) mod a 4
41 c**(a-1) mod a 1
35 a**(b-1) mod b 35
41 c**(b-1) mod b 3
35 a**(c-1) mod c 1
38 b**(c-1) mod c 1
37 -->
38 b**(a-1) mod a 1
39 c**(a-1) mod a 1
37 a**(b-1) mod b 37
39 c**(b-1) mod b 1
37 a**(c-1) mod c 4
38 b**(c-1) mod c 1
39 -->
38 b**(a-1) mod a 1
37 c**(a-1) mod a 4
39 a**(b-1) mod b 1
37 c**(b-1) mod b 37
39 a**(c-1) mod c 1
38 b**(c-1) mod c 1

```

.....: 78

les dg

```

5 -->
39 b**(a-1) mod a 1
73 c**(a-1) mod a 1
5 a**(b-1) mod b 25
73 c**(b-1) mod b 25
5 a**(c-1) mod c 1
39 b**(c-1) mod c 1
7 -->
39 b**(a-1) mod a 1
71 c**(a-1) mod a 1
7 a**(b-1) mod b 10
71 c**(b-1) mod b 10
7 a**(c-1) mod c 1
39 b**(c-1) mod c 1

```

```

11 -->
39 b**(a-1) mod a 1
67 c**(a-1) mod a 1
11 a**(b-1) mod b 4
67 c**(b-1) mod b 4
11 a**(c-1) mod c 1
39 b**(c-1) mod c 1
17 -->
39 b**(a-1) mod a 1
61 c**(a-1) mod a 1
17 a**(b-1) mod b 16
61 c**(b-1) mod b 16
17 a**(c-1) mod c 1
39 b**(c-1) mod c 1
19 -->
39 b**(a-1) mod a 1
59 c**(a-1) mod a 1
19 a**(b-1) mod b 10
59 c**(b-1) mod b 10
19 a**(c-1) mod c 1
39 b**(c-1) mod c 1
31 -->
39 b**(a-1) mod a 1
47 c**(a-1) mod a 1
31 a**(b-1) mod b 25
47 c**(b-1) mod b 25
31 a**(c-1) mod c 1
39 b**(c-1) mod c 1
37 -->
39 b**(a-1) mod a 1
41 c**(a-1) mod a 1
37 a**(b-1) mod b 4
41 c**(b-1) mod b 4
37 a**(c-1) mod c 1
39 b**(c-1) mod c 1

```

les non dg

```

3 -->
39 b**(a-1) mod a 0
75 c**(a-1) mod a 0
3 a**(b-1) mod b 9
75 c**(b-1) mod b 9
3 a**(c-1) mod c 69
39 b**(c-1) mod c 66
9 -->
39 b**(a-1) mod a 0
69 c**(a-1) mod a 0
9 a**(b-1) mod b 3
69 c**(b-1) mod b 3
9 a**(c-1) mod c 12
39 b**(c-1) mod c 3

```

```

13 -->
39 b**(a-1) mod a 0
65 c**(a-1) mod a 0
13 a**(b-1) mod b 13
65 c**(b-1) mod b 13
13 a**(c-1) mod c 26
39 b**(c-1) mod c 26
15 -->
39 b**(a-1) mod a 6
63 c**(a-1) mod a 9
15 a**(b-1) mod b 30
63 c**(b-1) mod b 30
15 a**(c-1) mod c 36
39 b**(c-1) mod c 9
21 -->
39 b**(a-1) mod a 9
57 c**(a-1) mod a 15
21 a**(b-1) mod b 12
57 c**(b-1) mod b 12
21 a**(c-1) mod c 42
39 b**(c-1) mod c 39
23 -->
39 b**(a-1) mod a 1
55 c**(a-1) mod a 1
23 a**(b-1) mod b 22
55 c**(b-1) mod b 22
23 a**(c-1) mod c 34
39 b**(c-1) mod c 31
25 -->
39 b**(a-1) mod a 16
53 c**(a-1) mod a 6
25 a**(b-1) mod b 1
53 c**(b-1) mod b 1
25 a**(c-1) mod c 1
39 b**(c-1) mod c 1
27 -->
39 b**(a-1) mod a 0
51 c**(a-1) mod a 0
27 a**(b-1) mod b 27
51 c**(b-1) mod b 27
27 a**(c-1) mod c 15
39 b**(c-1) mod c 42
29 -->
39 b**(a-1) mod a 1
49 c**(a-1) mod a 1
29 a**(b-1) mod b 22
49 c**(b-1) mod b 22
29 a**(c-1) mod c 22
39 b**(c-1) mod c 8

```

```

33 -->
39 b**(a-1) mod a 3
45 c**(a-1) mod a 12
33 a**(b-1) mod b 36
45 c**(b-1) mod b 36
33 a**(c-1) mod c 36
39 b**(c-1) mod c 36
35 -->
39 b**(a-1) mod a 11
43 c**(a-1) mod a 29
35 a**(b-1) mod b 16
43 c**(b-1) mod b 16
35 a**(c-1) mod c 1
39 b**(c-1) mod c 1
39 -->
39 b**(a-1) mod a 0
39 c**(a-1) mod a 0
39 a**(b-1) mod b 0
39 c**(b-1) mod b 0
39 a**(c-1) mod c 0
39 b**(c-1) mod c 0

```

.....: 80

les dg

```

7 -->
40 b**(a-1) mod a 1
73 c**(a-1) mod a 1
7 a**(b-1) mod b 23
73 c**(b-1) mod b 17
7 a**(c-1) mod c 1
40 b**(c-1) mod c 1
13 -->
40 b**(a-1) mod a 1
67 c**(a-1) mod a 1
13 a**(b-1) mod b 37
67 c**(b-1) mod b 3
13 a**(c-1) mod c 1
40 b**(c-1) mod c 1
19 -->
40 b**(a-1) mod a 1
61 c**(a-1) mod a 1
19 a**(b-1) mod b 19
61 c**(b-1) mod b 21
19 a**(c-1) mod c 1
40 b**(c-1) mod c 1
37 -->
40 b**(a-1) mod a 1
43 c**(a-1) mod a 1
37 a**(b-1) mod b 13
43 c**(b-1) mod b 27
37 a**(c-1) mod c 1
40 b**(c-1) mod c 1

```

les non dg

3 -->

40  $b^{**}(a-1) \bmod a$  1

77  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  27

77  $c^{**}(b-1) \bmod b$  13

3  $a^{**}(c-1) \bmod c$  25

40  $b^{**}(c-1) \bmod c$  37

5 -->

40  $b^{**}(a-1) \bmod a$  0

75  $c^{**}(a-1) \bmod a$  0

5  $a^{**}(b-1) \bmod b$  5

75  $c^{**}(b-1) \bmod b$  35

5  $a^{**}(c-1) \bmod c$  25

40  $b^{**}(c-1) \bmod c$  25

9 -->

40  $b^{**}(a-1) \bmod a$  7

71  $c^{**}(a-1) \bmod a$  1

9  $a^{**}(b-1) \bmod b$  9

71  $c^{**}(b-1) \bmod b$  31

9  $a^{**}(c-1) \bmod c$  1

40  $b^{**}(c-1) \bmod c$  1

11 -->

40  $b^{**}(a-1) \bmod a$  1

69  $c^{**}(a-1) \bmod a$  1

11  $a^{**}(b-1) \bmod b$  11

69  $c^{**}(b-1) \bmod b$  29

11  $a^{**}(c-1) \bmod c$  52

40  $b^{**}(c-1) \bmod c$  13

15 -->

40  $b^{**}(a-1) \bmod a$  10

65  $c^{**}(a-1) \bmod a$  10

15  $a^{**}(b-1) \bmod b$  15

65  $c^{**}(b-1) \bmod b$  25

15  $a^{**}(c-1) \bmod c$  55

40  $b^{**}(c-1) \bmod c$  40

17 -->

40  $b^{**}(a-1) \bmod a$  1

63  $c^{**}(a-1) \bmod a$  1

17  $a^{**}(b-1) \bmod b$  33

63  $c^{**}(b-1) \bmod b$  7

17  $a^{**}(c-1) \bmod c$  37

40  $b^{**}(c-1) \bmod c$  25

```

21 -->
40 b**(a-1) mod a 4
59 c**(a-1) mod a 16
21 a**(b-1) mod b 21
59 c**(b-1) mod b 19
21 a**(c-1) mod c 1
40 b**(c-1) mod c 1
23 -->
40 b**(a-1) mod a 1
57 c**(a-1) mod a 1
23 a**(b-1) mod b 7
57 c**(b-1) mod b 33
23 a**(c-1) mod c 16
40 b**(c-1) mod c 4
25 -->
40 b**(a-1) mod a 0
55 c**(a-1) mod a 0
25 a**(b-1) mod b 25
55 c**(b-1) mod b 15
25 a**(c-1) mod c 15
40 b**(c-1) mod c 25
27 -->
40 b**(a-1) mod a 25
53 c**(a-1) mod a 1
27 a**(b-1) mod b 3
53 c**(b-1) mod b 37
27 a**(c-1) mod c 1
40 b**(c-1) mod c 1
29 -->
40 b**(a-1) mod a 1
51 c**(a-1) mod a 1
29 a**(b-1) mod b 29
51 c**(b-1) mod b 11
29 a**(c-1) mod c 25
40 b**(c-1) mod c 19
31 -->
40 b**(a-1) mod a 1
49 c**(a-1) mod a 1
31 a**(b-1) mod b 31
49 c**(b-1) mod b 9
31 a**(c-1) mod c 1
40 b**(c-1) mod c 36
33 -->
40 b**(a-1) mod a 16
47 c**(a-1) mod a 31
33 a**(b-1) mod b 17
47 c**(b-1) mod b 23
33 a**(c-1) mod c 1
40 b**(c-1) mod c 1

```

```

35 -->
40 b**(a-1) mod a 30
45 c**(a-1) mod a 25
35 a**(b-1) mod b 35
45 c**(b-1) mod b 5
35 a**(c-1) mod c 10
40 b**(c-1) mod c 25
39 -->
40 b**(a-1) mod a 1
41 c**(a-1) mod a 4
39 a**(b-1) mod b 39
41 c**(b-1) mod b 1
39 a**(c-1) mod c 1
40 b**(c-1) mod c 1
41 -->
40 b**(a-1) mod a 1
39 c**(a-1) mod a 1
41 a**(b-1) mod b 1
39 c**(b-1) mod b 39
41 a**(c-1) mod c 4
40 b**(c-1) mod c 1

```

..... 84

les dg

```

5 -->
42 b**(a-1) mod a 1
79 c**(a-1) mod a 1
5 a**(b-1) mod b 17
79 c**(b-1) mod b 25
5 a**(c-1) mod c 1
42 b**(c-1) mod c 1
11 -->
42 b**(a-1) mod a 1
73 c**(a-1) mod a 1
11 a**(b-1) mod b 23
73 c**(b-1) mod b 19
11 a**(c-1) mod c 1
42 b**(c-1) mod c 1
13 -->
42 b**(a-1) mod a 1
71 c**(a-1) mod a 1
13 a**(b-1) mod b 13
71 c**(b-1) mod b 29
13 a**(c-1) mod c 1
42 b**(c-1) mod c 1

```

```

17 -->
42 b**(a-1) mod a 1
67 c**(a-1) mod a 1
17 a**(b-1) mod b 5
67 c**(b-1) mod b 37
17 a**(c-1) mod c 1
42 b**(c-1) mod c 1
23 -->
42 b**(a-1) mod a 1
61 c**(a-1) mod a 1
23 a**(b-1) mod b 11
61 c**(b-1) mod b 31
23 a**(c-1) mod c 1
42 b**(c-1) mod c 1
31 -->
42 b**(a-1) mod a 1
53 c**(a-1) mod a 1
31 a**(b-1) mod b 19
53 c**(b-1) mod b 23
31 a**(c-1) mod c 1
42 b**(c-1) mod c 1
37 -->
42 b**(a-1) mod a 1
47 c**(a-1) mod a 1
37 a**(b-1) mod b 25
47 c**(b-1) mod b 17
37 a**(c-1) mod c 1
42 b**(c-1) mod c 1
41 -->
42 b**(a-1) mod a 1
43 c**(a-1) mod a 1
41 a**(b-1) mod b 41
43 c**(b-1) mod b 1
41 a**(c-1) mod c 1
42 b**(c-1) mod c 1
43 -->
42 b**(a-1) mod a 1
41 c**(a-1) mod a 1
43 a**(b-1) mod b 1
41 c**(b-1) mod b 41
43 a**(c-1) mod c 1
42 b**(c-1) mod c 1

```

les non dg

```

3 -->
42 b**(a-1) mod a 0
81 c**(a-1) mod a 0
3 a**(b-1) mod b 33
81 c**(b-1) mod b 9
3 a**(c-1) mod c 0
42 b**(c-1) mod c 0

```



```

7 -->
42 b**(a-1) mod a 0
77 c**(a-1) mod a 0
7 a**(b-1) mod b 7
77 c**(b-1) mod b 35
7 a**(c-1) mod c 70
42 b**(c-1) mod c 42
9 -->
42 b**(a-1) mod a 0
75 c**(a-1) mod a 0
9 a**(b-1) mod b 39
75 c**(b-1) mod b 3
9 a**(c-1) mod c 36
42 b**(c-1) mod c 54
15 -->
42 b**(a-1) mod a 9
69 c**(a-1) mod a 6
15 a**(b-1) mod b 15
69 c**(b-1) mod b 27
15 a**(c-1) mod c 18
42 b**(c-1) mod c 39
19 -->
42 b**(a-1) mod a 1
65 c**(a-1) mod a 1
19 a**(b-1) mod b 31
65 c**(b-1) mod b 11
19 a**(c-1) mod c 61
42 b**(c-1) mod c 16
21 -->
42 b**(a-1) mod a 0
63 c**(a-1) mod a 0
21 a**(b-1) mod b 21
63 c**(b-1) mod b 21
21 a**(c-1) mod c 0
42 b**(c-1) mod c 0
25 -->
42 b**(a-1) mod a 21
59 c**(a-1) mod a 11
25 a**(b-1) mod b 37
59 c**(b-1) mod b 5
25 a**(c-1) mod c 1
42 b**(c-1) mod c 1
27 -->
42 b**(a-1) mod a 0
57 c**(a-1) mod a 0
27 a**(b-1) mod b 27
57 c**(b-1) mod b 15
27 a**(c-1) mod c 45
42 b**(c-1) mod c 54
29 -->
42 b**(a-1) mod a 1
55 c**(a-1) mod a 1
29 a**(b-1) mod b 29
55 c**(b-1) mod b 13
29 a**(c-1) mod c 36
42 b**(c-1) mod c 49

```

```

33 -->
42 b**(a-1) mod a 15
51 c**(a-1) mod a 27
33 a**(b-1) mod b 3
51 c**(b-1) mod b 39
33 a**(c-1) mod c 18
42 b**(c-1) mod c 30
35 -->
42 b**(a-1) mod a 14
49 c**(a-1) mod a 21
35 a**(b-1) mod b 35
49 c**(b-1) mod b 7
35 a**(c-1) mod c 0
42 b**(c-1) mod c 0
39 -->
42 b**(a-1) mod a 9
45 c**(a-1) mod a 36
39 a**(b-1) mod b 9
45 c**(b-1) mod b 33
39 a**(c-1) mod c 36
42 b**(c-1) mod c 36

```

.....: 88

les dg

```

5 -->
44 b**(a-1) mod a 1
83 c**(a-1) mod a 1
5 a**(b-1) mod b 37
83 c**(b-1) mod b 7
5 a**(c-1) mod c 1
44 b**(c-1) mod c 1
17 -->
44 b**(a-1) mod a 1
71 c**(a-1) mod a 1
17 a**(b-1) mod b 29
71 c**(b-1) mod b 15
17 a**(c-1) mod c 1
44 b**(c-1) mod c 1
29 -->
44 b**(a-1) mod a 1
59 c**(a-1) mod a 1
29 a**(b-1) mod b 13
59 c**(b-1) mod b 31
29 a**(c-1) mod c 1
44 b**(c-1) mod c 1
41 -->
44 b**(a-1) mod a 1
47 c**(a-1) mod a 1
41 a**(b-1) mod b 17
47 c**(b-1) mod b 27
41 a**(c-1) mod c 1
44 b**(c-1) mod c 1

```

les non dg

3 -->

44  $b^{**}(a-1) \bmod a$  1

85  $c^{**}(a-1) \bmod a$  1

3  $a^{**}(b-1) \bmod b$  27

85  $c^{**}(b-1) \bmod b$  17

3  $a^{**}(c-1) \bmod c$  81

44  $b^{**}(c-1) \bmod c$  21

7 -->

44  $b^{**}(a-1) \bmod a$  1

81  $c^{**}(a-1) \bmod a$  1

7  $a^{**}(b-1) \bmod b$  35

81  $c^{**}(b-1) \bmod b$  9

7  $a^{**}(c-1) \bmod c$  58

44  $b^{**}(c-1) \bmod c$  46

9 -->

44  $b^{**}(a-1) \bmod a$  1

79  $c^{**}(a-1) \bmod a$  4

9  $a^{**}(b-1) \bmod b$  25

79  $c^{**}(b-1) \bmod b$  19

9  $a^{**}(c-1) \bmod c$  1

44  $b^{**}(c-1) \bmod c$  1

11 -->

44  $b^{**}(a-1) \bmod a$  0

77  $c^{**}(a-1) \bmod a$  0

11  $a^{**}(b-1) \bmod b$  11

77  $c^{**}(b-1) \bmod b$  33

11  $a^{**}(c-1) \bmod c$  11

44  $b^{**}(c-1) \bmod c$  44

13 -->

44  $b^{**}(a-1) \bmod a$  1

75  $c^{**}(a-1) \bmod a$  1

13  $a^{**}(b-1) \bmod b$  41

75  $c^{**}(b-1) \bmod b$  3

13  $a^{**}(c-1) \bmod c$  64

44  $b^{**}(c-1) \bmod c$  46

15 -->

44  $b^{**}(a-1) \bmod a$  1

73  $c^{**}(a-1) \bmod a$  4

15  $a^{**}(b-1) \bmod b$  31

73  $c^{**}(b-1) \bmod b$  13

15  $a^{**}(c-1) \bmod c$  1

44  $b^{**}(c-1) \bmod c$  1

```

19 -->
44 b**(a-1) mod a 1
69 c**(a-1) mod a 1
19 a**(b-1) mod b 39
69 c**(b-1) mod b 5
19 a**(c-1) mod c 16
44 b**(c-1) mod c 4
21 -->
44 b**(a-1) mod a 4
67 c**(a-1) mod a 16
21 a**(b-1) mod b 21
67 c**(b-1) mod b 23
21 a**(c-1) mod c 1
44 b**(c-1) mod c 1
23 -->
44 b**(a-1) mod a 1
65 c**(a-1) mod a 1
23 a**(b-1) mod b 23
65 c**(b-1) mod b 21
23 a**(c-1) mod c 16
44 b**(c-1) mod c 1
25 -->
44 b**(a-1) mod a 21
63 c**(a-1) mod a 11
25 a**(b-1) mod b 5
63 c**(b-1) mod b 39
25 a**(c-1) mod c 58
44 b**(c-1) mod c 46
27 -->
44 b**(a-1) mod a 19
61 c**(a-1) mod a 4
27 a**(b-1) mod b 15
61 c**(b-1) mod b 29
27 a**(c-1) mod c 1
44 b**(c-1) mod c 1
31 -->
44 b**(a-1) mod a 1
57 c**(a-1) mod a 1
31 a**(b-1) mod b 3
57 c**(b-1) mod b 41
31 a**(c-1) mod c 49
44 b**(c-1) mod c 55
33 -->
44 b**(a-1) mod a 22
55 c**(a-1) mod a 22
33 a**(b-1) mod b 33
55 c**(b-1) mod b 11
33 a**(c-1) mod c 44
44 b**(c-1) mod c 11
35 -->
44 b**(a-1) mod a 16
53 c**(a-1) mod a 4
35 a**(b-1) mod b 19
53 c**(b-1) mod b 25
35 a**(c-1) mod c 1
44 b**(c-1) mod c 1

```

```
37 -->
44 b**(a-1) mod a 1
51 c**(a-1) mod a 1
37 a**(b-1) mod b 9
51 c**(b-1) mod b 35
37 a**(c-1) mod c 43
44 b**(c-1) mod c 49
39 -->
44 b**(a-1) mod a 25
49 c**(a-1) mod a 22
39 a**(b-1) mod b 7
49 c**(b-1) mod b 37
39 a**(c-1) mod c 8
44 b**(c-1) mod c 43
43 -->
44 b**(a-1) mod a 1
45 c**(a-1) mod a 1
43 a**(b-1) mod b 43
45 c**(b-1) mod b 1
43 a**(c-1) mod c 31
44 b**(c-1) mod c 1
45 -->
44 b**(a-1) mod a 1
43 c**(a-1) mod a 31
45 a**(b-1) mod b 1
43 c**(b-1) mod b 43
45 a**(c-1) mod c 1
44 b**(c-1) mod c 1
```