## Correction du devoir surveillé n°2

### Ex 1: Nombres premiers jumeaux (3 pts)

#### Nombres premiers jumeaux

On dit que p et p' sont des nombres premiers jumeaux, si p et p' sont des nombres premiers et p'=p+2. Par exemple p'=p+2 et p'=p+2 et

1. Donner la liste des couples de nombres premiers jumeaux  $(p,p^\prime)$  avec p<30.

Les nombres premiers inférieurs à 32 sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. Ainsi les couples (p, p + 2) de nombres premiers jumeaux sont : (3, 5), (5, 7), (11, 13), (17, 19), et (29, 31).

2. (101, 103) est-il un couple de nombres premiers jumeaux?

101 et 103 ne sont divisibles par aucun nombre premier inférieur ou égal à 10 qui est la valeur approchée par défaut de  $\sqrt{103}$ . Ainsi, ils sont tous deux premiers.

3. (839, 841) est-il un couple de nombres premiers jumeaux?

La racine carrée de 841 est 29. Certes 839 n'est divisible par aucun nombre premier inférieur ou égal à 29, mais  $841=29^2$  n'est donc pas premier.

### Ex2: Je sais travailler avec des fractions (8 pts)

Calculer et donner le résultat sous forme d'une fraction irréductible. Il faut donner toutes les étapes de calcul, et justifier que votre réponse est bien irréductible.

Pour la présentation, on ne mettra qu'un seul signe égal à chaque ligne, et on répétera la lettre juste avant à chaque fois.

#### Indices:

- $\bullet$  Pour le A, penser à la décomposition en facteurs premiers des dénominateurs.
- Pour le *B* penser au PGCD des dénominateurs.
- $\bullet$  Pour le C, la calculatrice est inutile.
- Pour le *D*, bien justifier que votre résultat est irréductible.

$$A = rac{2}{323} + rac{13}{323} imes rac{5}{91} \ A = rac{2}{17 imes 19} + rac{13 imes 5}{17 imes 19 imes 7 imes 13}$$

$$A = rac{2}{17 imes 19} + rac{5}{17 imes 19 imes 7}$$
 $A = rac{2 imes 7}{17 imes 19 imes 7} + rac{5}{17 imes 19 imes 7}$ 
 $A = rac{2 imes 7 + 5}{17 imes 19 imes 7}$ 
 $A = rac{19}{17 imes 19 imes 7}$ 
 $A = rac{1}{17 imes 7}$ 

Le numérateur de A est égal à 1, donc A est irréductible.

On calcule d'abord  $PGCD(11\,009,11\,227)$  avec l'algorithme d'Euclide :

$$11\,227 \div 11\,009 \mapsto (q=1, r=218)$$
 $11\,009 \div 218 \mapsto (q=50, r=109)$ 
 $218 \div 109 \mapsto (q=2, r=0)$ 

Le dernier diviseur est 109, c'est PGCD(11009, 11227).

On en déduit :  $11\,009 = 109 \times 101$  et  $11\,227 = 109 \times 103$ . Ainsi :

$$B = \frac{1}{11\,009} - \frac{1}{11\,227}$$

$$B = \frac{1}{109 \times 101} - \frac{1}{109 \times 103}$$

$$B = \frac{103}{109 \times 101 \times 103} - \frac{101}{109 \times 103 \times 101}$$

$$B = \frac{103 - 101}{109 \times 101 \times 103}$$

$$B = \frac{2}{109 \times 101 \times 103}$$

La seule simplification possible serait par 2 qui est la décomposition en facteurs premiers du numérateur, or les facteurs du dénominateurs sont tous impairs. Ainsi, B est irréductible.

$$C = rac{2^3 imes 3^5 imes 7}{11^2 imes 13^5} imes rac{13^2 imes 17^2}{2^2 imes 7^3 imes 11} \ C = rac{2^3 imes 3^5 imes 7 imes 13^2 imes 17^2}{11^2 imes 13^5 imes 2^2 imes 7^3 imes 11}$$

$$C = rac{2^{3-2} imes 3^5 imes 17^2}{11^{2+1} imes 13^{5-2} imes 7^{3-1}} \ C = rac{2 imes 3^5 imes 17^2}{11^3 imes 13^3 imes 7^2}$$

Il n'y a rien en commun dans la décomposition en facteurs premiers des numérateur et dénominateur, ainsi leur PGCD est égal à 1, et donc C est irréductible.

$$D = \frac{1}{p} - \frac{1}{p'}$$
, où  $p$  et  $p'$  sont des nombres premiers jumeaux.

$$D = rac{1}{p} - rac{1}{p+2}$$
 $D = rac{p+2}{p(p+2)} - rac{p}{p(p+2)}$ 
 $D = rac{p+2-p}{p(p+2)}$ 
 $D = rac{2}{p(p+2)}$ 

p et p+2 sont premiers, donc ni p=2, ni p+2=2, et donc p et p+2 sont des nombres premiers impairs et la seule simplification par p=2 est impossible, ainsi p=2 est irréductible.

# Ex 3 : Je sais faire des démonstrations (4 pts)

Pour chaque proposition, si elle est vraie donner une démonstration, si elle est fausse donner un contreexemple.

#### **Proposition 1**

Si p est un nombre premier, alors p+1 n'est pas un nombre premier.

**FAUSSE.** Avec p=2, on a p+1=3 qui est premier. Remarque : c'est le seul contre-exemple...

#### **Proposition 2**

Avec a, b, c trois entiers relatifs, si  $a \mid c$  et  $b \mid c$ , alors  $ab \mid c$ .

**FAUSSE.** Avec a=b=c=2, on a bien  $2\mid 2$ , mais pas  $4\mid 2$ .

#### **Proposition 3**

Avec a, b, c trois entiers relatifs, si  $a \mid c$  et  $b \mid c$ , alors  $ab \mid c^2$ .

**VRAIE.** On suppose que  $a,b,c\in\mathbb{Z}$ , avec  $a\mid c$  et  $b\mid c$ , il existe  $k,k'\in\mathbb{Z}$  tel que c=ka et c=k'b, on déduit  $c^2=ka\times k'b$ , et par commutativité de la multiplication  $c^2=(kk')\times ab$ , avec  $kk'\in\mathbb{Z}$ , de sorte que  $ab\mid c^2$ .

#### **Proposition 4**

Avec a, b, c trois entiers relatifs, si  $a \mid c$  et  $a \mid b$ , alors  $a \mid b + bc + c$ .

**VRAIE.** On suppose que  $a,b,c\in\mathbb{Z}$ , avec  $a\mid c$  et  $a\mid b$ , il existe  $k,k'\in\mathbb{Z}$  tel que c=ka et b=k'a, on déduit que b+bc+c=k'a+k'aka+ka=(k'+k'ak+k)a, avec  $(k'+k'ak+k)\in\mathbb{Z}$  de sorte que  $a\mid b+bc+c$ .

## Ex 4 : Je sais lire un script Python simple (2 pts)

Que fait le script suivant ? On cherchera d'abord ce que fait la fonction mystère, puis comment elle est utilisée.

```
def mystère(n, b):
    for d in range(2, b):
        if n%d == 0:
            return False
    return True

for p in range(2, 1000):
    if mystère(p, p) and mystère(p+2, 20) and (not mystère(p+2, p+2)):
        print(p, p+2, "pas le 2")
    if mystère(p, 20) and mystère(p+2, p+2) and (not mystère(p, p)):
        print(p, p+2, "pas le 1")
```

La fonction mystère teste s'il existe des diviseurs de n entre 2 inclus et b exclu.

On en déduit que :

- mystère(p, p) correspond à "p est premier".
- mystère(p+2, p+2) correspond à "p est premier".
- mystère(p+2, 20) correspond à "p+2 n'a aucun diviseur premier inférieur à 20".
- mystère(p, 20) correspond à "p n'a aucun diviseur premier inférieur à 20".

Le script recherche donc les nombres p entre 2 et 1000, tels que (p, p + 2) ne sont pas des nombres premiers jumeaux, mais presque...

## Ex 5: Prime or not prime? (3 pts)

1. On sait que  $10\,403$  n'est divisible par aucun nombre premier inférieur à 100.  $10\,403$  est-il premier ?

 $\sqrt{10\,403} pprox 102$ . On teste avec 101, et on trouve  $10\,403 = 101 imes 103$  qui n'est pas premier.

2. On sait que  $39\,989$  n'est divisible par aucun nombre premier inférieur à 200.  $39\,989$  est-il premier ?

 $\sqrt{39\,989} pprox 200$ . On en déduit que  $39\,989$  est premier.

3. p>3, et (p,p+2) sont des nombres premiers jumeaux. p+4 est-il un nombre premier ? (On pourra tester les trois cas de p modulo 3.)

On suppose que p+4 est premier.

- Si p modulo 3 est égal à 0, avec p premier, on déduit p divisible par 3, donc p=3, ce qui entre en contradiction avec p>3. Ce cas est impossible.
- Si p modulo 3 est égal à 1, alors p=3k+1, avec  $k\in\mathbb{Z}$ , de sorte que p+2=3k+1+2=3k+3=3(k+1) avec  $(k+1)\in\mathbb{Z}$  de sorte que p+2 est divisible par 3, mais premier en même temps, donc p+2=3 et donc p=1 ce qui contredit p>3. Ce cas est impossible.
- Si p modulo 3 est égal à 2, alors p=3k+2, avec  $k\in\mathbb{Z}$ , de sorte que p+4=3k+2+4=3k+6=3(k+2) avec  $(k+2)\in\mathbb{Z}$  de sorte que p+4 est divisible par 3, mais premier en même temps, donc p+4=3 et donc p=-1 ce qui contredit p>3. Ce cas est impossible.

On a raisonné par disjonction des cas, et dans tous les cas on a une contradiction, ainsi p+4 n'est pas premier.

Fin.