1 (⋆) Décomposer les nombres 10080 et 11880 en produit de facteurs premiers. En déduire leur PGCD et leur PPCM.

2 (⋆) En utilisant l'algorithme d'Euclide :

1. déterminer le PGCD de 1665 et 962
2. Calculer le PPCM de 377 et 464
3. Simplifier la fraction $\frac{1240}{1116}$
4. Trouver une relation de Bezout entre 23 et 29

3 (⋆) Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $2x+1 \equiv 4\,[7]$
2. $3x \equiv 9\,[12]$
3. $3x \equiv 10\,[12]$
4. $x^2-3x+2 \equiv 0\,[8]$
5. $x^2-3x+2 \equiv 0\,[7]$
6. $x^3 \equiv 1\,[7]$

4 (⋆) Soit $x \in \mathbb{N}$ un carré parfait (ie le carré d'un autre entier). Montrer que

1. x pair $\Rightarrow x \equiv 0\,[4]$
2. x impair $\Rightarrow x \equiv 1\,[8]$

5 (⋆) Soient a et n des entiers naturels non nuls.

1. Montrer qu'il existe des entiers naturels $i \neq j$ tels que $a^i \equiv a^j\,[n]$
2. Dans cette question on suppose a et n premiers entre eux. Montrer qu'il existe $r \in \mathbb{N}^*$ tel que $a^r \equiv 1\,[n]$. Que dire de la suite $(a^k)_{k\in\mathbb{N}}$?
3. Cette propriété est-elle encore vraie si a et n ne sont pas premiers entre eux ?

6 (⋆)

1. Montrer que le produit de deux entiers consécutifs est divisible par 2.
2. (⋆⋆) Généraliser : pour $k \in \mathbb{N}^*$, montrer que le produit de k nombres entiers consécutifs est divisible par $k!$

RÉPONSE : $n(n+1)\cdots(n+k-1) = k!\binom{n+k-1}{k}$

7 (⋆⋆) Écrire en langage Python :

1. Une fonction qui calcule le PGCD de deux entiers par l'algorithme d'Euclide
2. Une fonction qui calcule le PPCM de deux entiers
3. Une fonction qui teste si un entier donné est premier
4. Une fonction qui calcule le plus petit diviseur premier d'un entier donné

RÉPONSE :

1.
```
#entiers a et b supposés positifs
def pgcd(a,b):
    u=a
    v=b
    while v>0:
        r=u%v
        v=u
        u=r
    return(u)
```

2.
```
#le ppcm de (a,b) est a'b avec a'=a/pgcd(a,b)
def ppcm(a,b):
    if a==0 or b==0:
        return(0)
    else:
        d=pgcd(a,b)
        a1=a/d
        return(a1*b)
```

3. On vérifie si p est premier par le crible d'Eratosthène, en cherchant un diviseur de p inférieur ou égal à $\sqrt{p}$

```
def test_primalite(p): #p supposé >1
    d=2
    rac=p**0.5
    while d<=rac:
        if p%d==0: #si d divise p
            return(False)
        else:
            d=d+1
    return(True)
```

4. Là encore il suffit de chercher un diviseur de n qui est $\leqslant \sqrt{n}$

```
def diviseur_premier(n): #n supposé >1
    d=2
    rac=n**0.5
    while d<=rac:
        if n%d==0: #si d divise n
            return(d)
        else:
            d=d+1
    return(n)
```

8 ($\star\star$) Soient x et y des entiers premiers entre eux. Montrer que $2x+3y$ et $5x+7y$ sont premiers entre eux

Réponse : Soit $d>0$ un diviseur commun de $2x+3y$ et $5x+7y$. Alors d divise $-7.(2x+3y)+3.(5x+7y)=x$. De même on montre $d|y$. Donc $d|x\wedge y=1$. Donc $d=1$ et $2x+3y$ et $5x+7y$ sont premiers entre eux

9 ($\star\star$)

1. Déterminer un couple d'entiers (x_0,y_0) tel que $15x_0+17y_0=1$
2. En déduire tous les couples $(x,y)\in\mathbb{Z}^2$ tels que $15x+17y=1$

Réponse :

1. En remontant l'algorithme d'Euclide sur $(15,17)$ on trouve $x_0=8$ et $y_0=-7$
2. Soit (x,y) une solution, alors $15(x-x_0)=17(y_0-y)$. En particulier $15|17(y_0-y)$. Or $15\wedge 17=1$ donc (lemme de Gauss) $15|y_0-y$, ie $y=y_0-15k$ avec $k\in\mathbb{Z}$. On trouve alors $x=x_0+17k$. Réciproquement, pour tout $k\in\mathbb{Z}$, le couple (x_0+17k,y_0-17k) est solution

10 ($\star\star$) Quel est le reste de la division euclidienne de 2020^{2020} par 7 ? et de $2020^{2020^{2020}}$ par 7 ?

Réponse :

* $2020\equiv 4\ [7]$ donc $2020^{2020}\equiv 4^{2020}\ [7]$. Ensuite $4^3\equiv 1\ [7]$ et $2020\equiv 1\ [3]$ donc $4^{2020}\equiv 4^1=4\ [7]$
* $2020^{2020}\equiv 1^{2020}=1\ [3]$ donc $2020^{2020}\equiv 4^1=4\ [7]$

11 ($\star\star$)

1. Soit x le réel de développement décimal $x=0,1212121212\cdots$. Montrer que x est un nombre rationnel. On admettra que $x=\lim x_n$ où on a posé $x_1=0,12$, $x_2=0,1212$, $x_3=0,121212$ etc

2. Faire de même avec $y = 0,5121121121121121...$

RÉPONSE :

1. $x = \frac{4}{33}$
2. On pose $y_n = 0,5(121)(121)...(121)$ où le bloc 121 apparait n fois, et on écrit :

$$y_n = 0,5 + 121.10^{-4} + 121.10^{-7} + \cdots + 121.10^{-3n-1} = \frac{1}{2} + \frac{121}{10^4}\sum_{k=0}^{n-1} 10^{-3k}$$

$$= \frac{1}{2} + \frac{121}{10^4}\frac{1-10^{-3n}}{1-10^{-3}} = \frac{1}{2} + \frac{121}{9990}(1-10^{-3n})$$

donc $y = \lim y_n = \frac{1}{2} + \frac{121}{9990} = \frac{10232}{19980} \in \mathbb{Q}$

12 ($\star\star\star$) Soit p un nombre premier.

1. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$
2. En déduire : $\forall (a,b) \in \mathbb{Z}^2 \quad (a+b)^p \equiv a^p + b^p \,[p]$
3. Démontrer le petit théorème de Fermat : $\forall a \in \mathbb{Z}^2 \quad a^p \equiv a \,[p]$ (indication : écrire $a^p = (1+1+\cdots+1)^p$ et utiliser la question précédente)

13 ($\star\star$) On cherche tous les entiers x solutions du système (S) : $\begin{cases} x \equiv 2 \ [11] \\ x \equiv 6 \ [19] \end{cases}$

1. Soit x une solution de (S), montrer qu'il existe $k \in \mathbb{Z}$ tel que $x = 2 + 11k$ et $11k \equiv 4 \ [19]$
2. Déterminer un entier $u \in [\![0, 18]\!]$ tel que $11u \equiv 1 \ [19]$, et montrer que $k \equiv 4u \,[19]$
3. En déduire toutes les solutions de (S).

RÉPONSE :

1. La première équation donne $x = 2 + 11k$ avec $k \in \mathbb{Z}$. La deuxième équation donne alors $2 + 11k \equiv 6 \,[19]$, donc $11k \equiv 4 \,[19]$
2. On trouve u en cherchant une relation de Bezout entre 11 et 19. On trouve $7 \times 11 - 4 \times 19 = 1$, donc $u = 7$ convient.
   De la relation $11k \equiv 4 \,[19]$ on déduit $u.11.k \equiv 4u \,[19]$ donc $k \equiv 4u \equiv 9 \,[19]$
3. On peut écrire $k = 9 + 19p$, $p \in \mathbb{Z}$, donc $x = 2 + 11k = 101 + 209p$. Réciproquement ces entiers sont bien solutions du système.

14 ($\star\star\star$) Pour tout $n \in \mathbb{N}^*$ on note $\tau(n)$ le nombre de diviseurs positifs de n.

1. Calculer $\tau(n)$ pour $n = p$ premier, puis pour $n = p^\alpha$ ($\alpha \in \mathbb{N}$)
2. Montrer que $\forall (m,n) \in (\mathbb{N}^*)^2 \quad m \wedge n = 1 \Rightarrow \tau(mn) = \tau(m)\tau(n)$
3. En déduire que pour tout $n \in \mathbb{N}^*$, $\tau(n) = \prod_{p \in \mathcal{P}} (v_p(n) + 1)$ où $v_p(n)$ est l'exposant de p dans la décomposition de n en produit de facteurs premiers.

RÉPONSE :

1. $\tau(p) = 2$, $\tau(p^\alpha) = \alpha + 1$ (les diviseurs de p^α sont les entiers p^j, avec $0 \leq j \leq \alpha$)
2. Soient m, n premiers entre eux. Un diviseur de mn s'écrit de façon unique comme le produit d'un diviseur de m et d'un diviseur de n. Donc $\tau(mn) = \tau(m)\tau(n)$
3. Il suffit de décomposer n en produit de facteurs premiers.

15 ($\star\star\star$) Soit $a \in \mathbb{N}^*$ et $n \in \mathbb{N}$, $n > 1$.

1. Montrer que $a-1$ divise $a^n - 1$
2. En déduire que $a^n - 1$ premier $\Rightarrow a = 2$ et n premier.
3. Vérifier que la réciproque est fausse.
   Les nombres premiers de la forme $2^n - 1$ sont appelés nombres de Mersenne

RÉPONSE :

1. $a^n - 1 = (a-1)(1 + a + \cdots + a^{n-1})$
2. Supposons $a^n - 1$ premier. Alors $a - 1$ divise $a^n - 1$ et $a - 1 < a^n - 1$ (il faut supposer $n > 1$ dans cette question) donc $a - 1 = 1$ donc $a = 2$.
   Supposons n composé : $n = pq$ avec $p > 1$ et $q > 1$. Alors $2^n - 1 = (2^p)^q - 1$ serait divisible par $2^p - 1$, donc $2^p - 1 = 1$: absurde. Donc n est premier
3. $2^{11} - 1$ est divisible par 23

16 ($\star\star\star$) Soient $a, b \in \mathbb{N}^*$, $a > 1$

1. Montrer que si b est impair, alors $a^b + 1$ est divisible par $a + 1$.
2. En déduire que si $a^b + 1$ est premier, alors a est pair et $b = 2^n$ avec $n \in \mathbb{N}$
3. On pose $F_n = 2^{2^n} + 1$. Vérifier que F_n est premier pour $n \leqslant 4$. *Les nombres premiers de la forme $2^{2^n} + 1$ sont appelés nombres de Fermat. Euler a montré que F_5 n'est pas premier. Une conjecture non démontrée affirme que F_n est premier si et seulement si $n \leqslant 4$*

RÉPONSE :

1. Si $b$est impair $a^b + 1 = a^b - (-1)^b = (a+1)(a^{b-1} - a^{b-2} + \cdots + (-1)^{b-1})$
2. Supposons $a^b + 1$ premier. Si a est impair alors $a^b + 1$ est pair, donc $a^b + 1 = 2$: absurde. Donc a est pair. Écrivons $b = 2^n c$ où c est impair.D'où $a^b + 1 = (a^{2^n})^c + 1$. D'après la question précédente ce nombre est divisible par $a^{2^n} + 1 > 1$, donc $a^b + 1 = a^{2^n} + 1$ donc $b = 2^n$