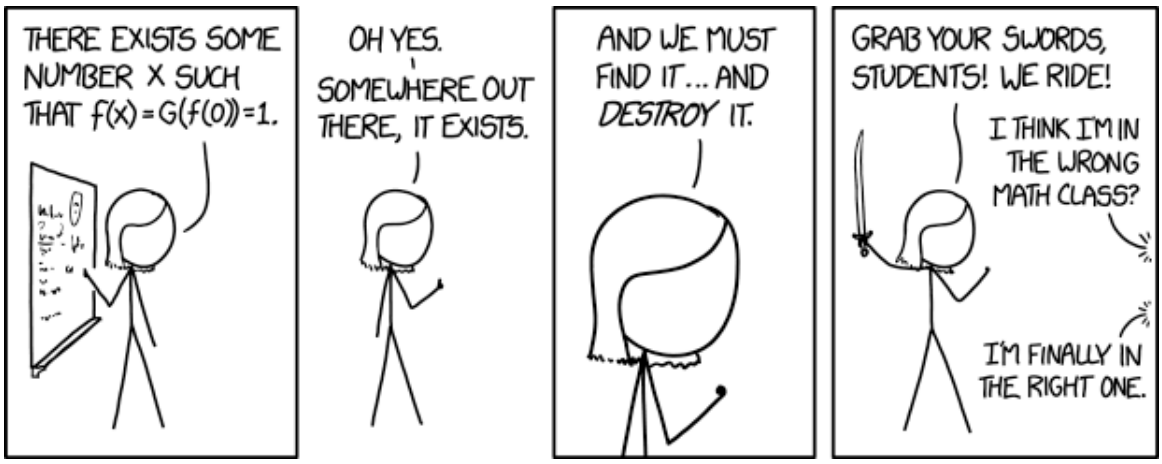
CERI — Licence — INFO — Semestre 2 — Mathématiques discrètes — 3 mai 2018

Évaluation écrite – Arithmétique
Durée 1h20

Seule la calculatrice de type collège ***(non programmable)*** *est autorisée.*

Il est inutile de finir tout le sujet pour avoir la note maximale.



https://xkcd.com/1856/

Dans tout le devoir, vous pourrez utiliser sans preuve que :
— 257 et 1 000 000 009 sont des nombres premiers.

I] Je sais calculer un PGCD (10 points)

1. Donner la décomposition en facteurs premiers de $A = 1326$ et $B = 75000000675$. *Inutile de justifier ici.*
2. Calculer PGCD(1326, 1482) avec deux méthodes différentes. *On attend le nom des méthodes et une présentation correcte des calculs, ainsi qu'une phrase de conclusion.*
3. Calculer PGCD(98 882, 99 862). *Donner quelques détails de calculs, le résultat seul ne rapporte aucun point.*
4. Calculer PGCD(1 000 000 009, 2 000 000 018). *Donner quelques détails sur votre méthode.*

II] Je sais trouver la liste des diviseurs (7 points)

1. Donner la liste des diviseurs de 930. *On attend une bonne présentation des calculs.*
2. On a demandé à Alice et à Bob de faire un script qui donne la somme des diviseurs d'un entier naturel non nul.
   Ces scripts sont faux, trouver la ou les erreurs. Les erreurs sont de petits oublis ou des caractères échangés. *On n'attend pas une réécriture, ni votre version. On attend que les petites erreurs soient identifiées et corrigées.*

```python
def somDiv(n):
    "Somme des diviseurs de n, par Alice"
    S = 0
    for x in range(1, n):
        if x*x>n: break
        if n%x == 0:
           S += x + x//n
           if x*x == n:
               S -= x
    return S
```

```python
def somDiv(n):
    "Somme des diviseurs de n, par Bob"
    S = 0
    for x in range(1, n+1):
        if x%n == 0:
           S += n
    return S
```

II] Je sais déterminer si un nombre est premier (8 points)

1. Pour chacun des nombres suivants, dire s'il est composé ou premier. *Justifier le.*

$$n_1 = 221,\ n_2 = 139,\ n_3 = 90\,000\,000\,000\,000\,300\,000\,000\,081,\ n_4 = 102\,509\,874\,063\,005$$

2. Xerk possède la liste des nombres premiers jusqu'à 65537, et il assure qu'aucun d'eux ne divise ni n_5, ni n_6. *On peut le croire !*

   Les nombre $n_5 = 4\,296\,409\,193$ et $n_6 = 4295098349$ sont-ils premiers ou non ? *Justifier.*
3. Les nombres premiers jumeaux sont des nombres premiers de la forme $(p, p+2)$, comme par exemple : $(5,7)$, ou bien $(11,13)$. Est-il possible d'avoir des nombres premiers triplets, de la forme $(p, p+2, p+4)$? *Justifier.*
4. Donner le nom d'une méthode qui détermine tous les nombres premiers dans un intervalle.

III] VRAI ou FAUX ? (11 points)

Pour cet exercice, il est inutile de justifier. Présenter ses réponses sur deux colonnes bien alignées : une avec le numéro de la question, l'autre avec VRAI ou FAUX.

1. $9197 = 17 \times 540 + 17$.
2. 9197 modulo 540 est égal à 17.
3. 9197 modulo 17 est égal à 17.
4. Avec $a, b, c, u, v \in \mathbb{Z}$, si $a \mid b$ et $a \mid c$, alors $a \mid ub + vc$.
5. Pour $a \in \mathbb{Z}$, on $a \wedge 1 = 1$, même pour $a = 0$.
6. Pour $k \in \mathbb{Z}$, on a $7(3k+1) - 3(7k+2) = 1$.
7. Pour $k \in \mathbb{Z}$, on a $(3k+1) \wedge (7k+2) = 1$.
8. Pour $k \in \mathbb{Z}$, 3 est un inverse de $7k+2$, modulo $3k+1$.
9. Pour $k \in \mathbb{Z}$, 7 est un inverse de $3k+1$, modulo $7k+2$.
10. $2^7 \times 7^2$ est la décomposition en facteurs premiers de 6872.
11. $2^7 \times 51$ est la décomposition en facteurs premiers de 6528.

IV] Je sais utiliser une formule (6 points)

On rappelle que les fonctions nombre de diviseurs, somme des diviseurs, et indicatrice d'Euler sont des fonctions arithmétiques multiplicatives. Elles vérifient donc en tant que f :

$$\forall u, v \in \mathbb{N}^*, u \wedge v = 1 \implies f(uv) = f(u)f(v)$$

On rappelle de plus, pour p un nombre premier, et $e \in \mathbb{N}^*$, que :

— Le nombre de diviseurs de p^e est $e+1$.

— La somme des diviseurs de p^e est $\dfrac{p^{e+1}-1}{p-1}$.

— L'indicatrice d'Euler de p^e est $p^{e-1}(p-1)$.

1. Vérifier que $362\,880 = 2^e \times 3^4 \times 5 \times 7$, où e est un entier à déterminer.
2. Vérifier que le nombre de diviseurs de 362 880 est égal à 160.
3. Calculer la somme des diviseurs de 362 880.
4. Calculer l'indicatrice d'Euler de 362 880.

V] Je fais de l'arithmétique modulaire simple (5 points)

Toutes les réponses doivent être justifiées.

1. Montrer que $3^2 \equiv -1 \pmod{10}$.
2. En déduire que $3^4 \equiv 1 \pmod{10}$.
3. Montrer que $403 \equiv 3 \pmod{4}$.
4. Quel est le dernier chiffre de 3^{403} ?
5. Quel est le dernier chiffre de $3^{(403^{42})}$?

VI] Je sais évaluer un polynôme (5 points)

On considère le polynôme $P(x) = 3x^5 - 2x^4 + 5x^2 + x - 1$, on ne s'intéresse qu'aux résultats modulo 257.

1. Vérifier que $P(0) \bmod 257 = 256$.
2. Calculer $P(1) \bmod 257$.
3. Calculer $P(111) \bmod 257$.

VII] Je sais résoudre des équations simples (5 points)

1. Résoudre l'équation où $x \in \mathbb{Z}$:

$$6x \equiv 12 \pmod{27}$$

2. Résoudre le système où $x, y \in \mathbb{Z}$:

$$\begin{cases} x + 2y \equiv 6 \pmod{7} \\ 5x + 4y \equiv 3 \pmod{7} \end{cases}$$

VIII] Je sais calculer un inverse modulaire (3 points)

Montrer que 31 est inversible modulo 100, et proposer un inverse.

Fin du sujet