NOM :
Prénom :
Nbre de feuilles rendues :

Université de Rennes 1
M1 MEFF Maths (2016-2017)
Algèbre, Géométrie, Algorithmique II
Contôle continu 4 (90 minutes + 30 minutes si tiers-temps)

On rédige sur cette feuille et on poursuit sur des feuilles supplémentaires. On numérote toutes les feuilles et on indique son nom sur chacune d'elles. Les documents et les appareils électroniques sont interdits. Une attention particulière sera portée à la qualité de la rédaction.

Exercice 1. (4 pts)
1/ Donner en justifiant une injection de $\mathbf{Q}$ dans $\mathbf{Z}$.
2/ Donner en justifiant une loi de composition interne commutative et non associative.
3/ Montrer que si $P \in \mathbf{Z}[X]$ alors $P\mathbf{Z}[X] \neq \{(2+X^2)U + 3XV; U, V \in \mathbf{Z}[X]\}$.
4/ Soit $n \in \mathbf{N}$. Donner un algorithme de calcul des nombres premiers inférieurs ou égaux à n.

Exercice 2. (1 pt)
Soit $n \in \mathbf{N}$. Montrer que si n est le carré d'un nombre rationnel ce rationnel est un entier.

Exercice 3. (3 pts)
Soit $p \in \mathbf{N}$ supposé premier.
1/ Montrer que si $k \in \{1, ..., p-1\}$ alors $\dfrac{p!}{k!(p-k)!}$ est un entier naturel divisible par p.
2/ Montrer par récurrence sur $n \in \mathbf{N}$ que p divise $n^p - n$.
3/ En déduire que si $n \in \mathbf{N}$ n'est pas divisible par p alors $n^{p-1} \equiv_p 1$.

Exercice 4. (7 pts)
1/ Montrer qu'il existe un nombre infini de nombres premiers.
2/ Montrer que si $p_1, ..., p_n$ sont des nombres premiers tous congrus à 3 modulo 4 alors il existe un nombre premier p qui leur est différent, qui est congru à 3 modulo 4 et qui divise $1 + p_1 \cdot ... \cdot p_n$.
3/ En déduire qu'il existe un nombre infini de nombre premiers congrus à 3 modulo 4.
4/ Soient $p_1, ..., p_n$ des nombres premiers tous congrus à 1 modulo 4 et soit p un nombre premier. On pose $N = p_1 \cdot ... \cdot p_n$ et on suppose que p divise $1 + N^2$.
a/ Vérifier que $N^2 \equiv_p -1$ et montrer que si p est congru congru à 3 modulo 4, c'est à dire que s'il existe $k \in \mathbf{N}$ tel que $p = 4k + 3$, alors $N^{p-1} \equiv_p -1$.
b/ Montrer que p ne peut pas être congru à 3 modulo 4. On pourra utiliser ici le petit théorème de Fermat qui dit que si p est premier et si a est un entier non multiple de p alors $a^{p-1} \equiv_p 1$.
c/ En déduire que p est congru à 1 modulo 4.
5/ En déduire qu'il existe un nombre infini de nombre premiers congrus à 1 modulo 4.

Exercice 5. (3 pts)
Soit $u \in]0,1[\backslash \mathbf{Q}$ un nombre irrationnel compris entre 0 et 1 et soit $G = \{nu + m; n, m \in \mathbf{Z}\}$. On considère la suite $(u_n)_{n \in \mathbf{N}}$ de premier terme $u_0 = u$ et telle que si $n \in \mathbf{N}$ alors u_{n+1} est le plus petit des deux nombres $R = 1 - u_n \cdot \text{partie entière}(1/u_n)$ et $u_n - R$.
1/ Vérifier que la suite $(u_n)_{n \in \mathbf{N}}$ est une suite bien définie d'irrationnels appartenant à $G \cap]0,1[$.
2/ Vérifier que si $n \in \mathbf{N}$ alors $0 \leq u_{n+1} \leq u_n/2$ et en déduire que la suite $(u_n)_{n \in \mathbf{N}}$ tend vers 0.
3/ Soit $x \in \mathbf{R}$ et $\varepsilon \in]0, +\infty)$. Montrer qu'il existe $a, b \in G$ tels que $a < x < b$ et $b - a < \varepsilon$.

Exercice 6. (2 pts)
1/ Soient $a, b \in \mathbf{N}$. Donner en justifiant un algorithme permettant de trouver $u, v \in \mathbf{Z}$ tels que $ua + vb = pgcd(a, b)$.
2/ Résoudre dans $\mathbf{Z}^2$ l'équation $97u + 41v = 1$.