UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 1

Examen terminal
mercredi 17 décembre 2014

Les documents de cours, calculatrices et téléphones portables ne sont pas autorisés.
Le sujet comporte six exercices.
Toutes les réponses doivent être justifiées.
Le barème est donné à titre indicatif.

Exercice 1 *3 points*

Soient p et q deux entiers naturels. On considère la proposition P :

$$pq \text{ est divisible par } 6 \Longrightarrow (p \text{ divisible par } 6 \text{ ou } q \text{ divisible par } 6).$$

1. Écrire la contraposée de cette proposition.
On considère maintenant la proposition Q :

$$\forall p \in \mathbf{N}, \forall q \in \mathbf{N},\ pq \text{ est divisible par } 6 \Longrightarrow (p \text{ divisible par } 6 \text{ ou } q \text{ divisible par } 6).$$

2. Écrire la négation de cette proposition Q.
3. La proposition Q est-elle vraie ou fausse ? Justifier.

Éléments de solution 1

1. *La contraposée de P est*

$$(p \text{ n'est pas divisible par } 6 \text{ et } q \text{ n'est pas divisible par } 6) \Longrightarrow pq \text{ n'est pas divisible par } 6.$$

2. *La négation de Q s'écrit*

$\exists p \in \mathbf{N}, \exists q \in \mathbf{N}$, *$pq$ est divisible par 6 et (p n'est pas divisible pas par 6 et q n'est pas divisible par 6).*

3. *La proposition Q est fausse. En effet, prenons $p = 2$ et $q = 3$. Alors $pq = 6$ est divisible par 6 et p n'est pas divisible par 6 et q n'est pas divisible par 6. On a montré que non Q est vraie.*

Exercice 2 *3 points*

Soient E et F deux ensembles et $f : E \to F$ une application quelconque. On se donne enfin $A \subset E$ et $B \subset F$.
1. Énoncer les définitions d'image directe et d'image réciproque.
2. Prouver que $f^{-1}(B) \cap A \subset f^{-1}(B \cap f(A))$. Montrer qu'on n'a pas toujours égalité.

Éléments de solution 2

1. *L'image directe d'un sous-ensemble A de E est l'ensemble noté $f(A)$ et défini par $f(A) = \{f(x)\,;\, x \in A\} = \{y \in F\,;\, \exists x \in A, y = f(x)\}$.*
L'image réciproque d'un sous-ensemble B de F est l'ensemble noté $f^{-1}(B)$ et défini par $f^{-1}(B) = \{x \in E\,;\, f(x) \in B\}$.
2. *Soit $x \in f^{-1}(B) \cap A$. Montrons que $x \in f^{-1}(B \cap f(A))$.*
Comme $x \in f^{-1}(B) \cap A$, alors $f(x) \in B$ et $x \in A$ et, si $x \in A$, alors $f(x) \in f(A)$. On en déduit que $f(x) \in B \cap f(A)$. Autrement dit, $x \in f^{-1}(B \cap f(A))$.
On n'a pas toujours égalité. En effet, soit $x \in f^{-1}(B \cap f(A))$. Alors $f(x) \in B$ et $f(x) \in f(A)$. Or $f(x) \in f(A)$ signifie qu'il existe un élément de A dont l'image est égale à $f(x)$. Mais rien ne dit

que cet élément soit x (ce serait le cas si f est injective). Construisons alors un contre-exemple. Soit $E = F = \{0; 1\}$ et f l'application constante qui à $x \in E$, associe $0 \in F$. Posons $A = \{0\}$ et $B = \{0; 1\}$. Alors
$f^{-1}(B) = \{0; 1\}$ et $f^{-1}(B) \cap A = \{0\}$
$f(A) = \{0\}$, donc $B \cap f(A) = \{0\}$ et $f^{-1}(B \cap f(A)) = \{0; 1\}$.
Il n'y a donc pas égalité.

Exercice 3

3 points

1. L'entier 193 est-il premier ?
2. Énoncer le théorème de décomposition des entiers naturels en produit de facteurs premiers.
3. Démontrer par l'absurde que $\sqrt{1737}$ n'est pas un entier.
4. Énoncer le petit théorème de Fermat.
5. Quel est le reste de la division euclidienne de 23^{384} par 193 ?

Éléments de solution 3

1. *D'après les critères de divisibilité par 2, 3, 5 et 11, 193 n'est pas divisible par 2, 3, 5 ou 11. De plus,* $193 = 7 \times 27 + 4$ *donc 193 n'est pas divisible par 7 et* $193 = 13 \times 14 + 11$ *donc 193 n'est pas divisible par 13. L'entier premier qui suit 13 est 17, or* $17^2 > 193$. *On a donc montré que 193 est premier.*
2. *Soit n un entier supérieur ou égal à 2. Alors on peut écrire n sous la forme $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ où les p_i sont des entiers premiers distincts deux à deux et α_i des entiers naturels non nuls. Si l'on suppose de plus $p_1 < p_2 < \cdots < p_k$, alors cette décomposition est unique.*
3. *Supposons que $\sqrt{1\,737}$ soit un entier. Comme il est supérieur ou égal à 2, on peut écrire $\sqrt{1737} = \prod_{i=1}^{k} p_i^{\alpha_i}$ et on en déduit que $1737 = \prod_{i=1}^{k} p_i^{2\alpha_i}$.*
Cherchons la décomposition de $1\,737$ en produit de facteurs premiers. La somme des chiffres de 1737 est divisible par 9, donc $1\,737$ est divisible par 9 et on a $1\,737 = 9 \times 193$. Or, d'après la question 1, l'entier 193 est premier. Donc la décomposition de $1\,737$ est $3^2 \times 193$. Les puissances ne sont pas paires. Donc $\sqrt{1737}$ n'est pas un entier.
4. *Soit p un entier premier. Alors pour tout entier x premier avec p, on a $x^{p-1} \equiv 1 \pmod{p}$. Et pour tout entier x, $x^p \equiv x \pmod{p}$.*
5. *Comme 193 est premier et que 23 est premier avec 193 (car ils sont tous les deux premiers), on a, d'après le petit théorème de Fermat, $23^{192} \equiv 1 \pmod{193}$. En mettant au carré, on obtient $23^{2\times 192} = 23^{384} \equiv 1 \pmod{193}$. On en déduit que le reste de la division euclidienne de 23^{384} par 193 est 1.*

Exercice 4

3 points

On définit une application de $\mathbb{N}$ dans $\mathbb{N}$ par $f(n) = \text{pgcd}(42, n)$ pour tout entier naturel n.
1. Calculer $f(0)$, $f(2)$, $f(10)$ et $f(5)$. L'application f est-elle injective ?
2. L'application f est-elle surjective ? Déterminer $f(\mathbb{N})$.

Éléments de solution 4

1. *On a $f(0) = 42$, $f(2) = 2$ car 2 divise 42, $f(10) = 2$ car $10 = 2 \times 5$ et $42 = 2 \times 3 \times 7$ et $f(5) = 1$.*
2. *On a $f(2) = f(10)$ et $10 \neq 2$ donc f n'est pas injective.*
3. *Soit $y = 0$, alors y ne peut pas être le* pgcd *de 42 et d'un autre entier, donc f n'est pas surjective.*

Par définition, $f(\mathbb{N}) = \{y \in \mathbb{N} \mid \exists n \in \mathbb{N},\ y = \text{pgcd}(42, n)\}$. Nécessairement, y est un diviseur de $42 = 2 \times 3 \times 7$. On en déduit que $f(\mathbb{N}) \subset E = \{1, 2, 3, 6, 7, 14, 21, 42\}$. Or, si $y \in E$, alors $y = \text{pgcd}(42, y)$ car y divise 42. On a donc $f(\mathbb{N}) = \{1, 2, 3, 6, 7, 14, 21, 42\}$.

Exercice 5

5 points

1. Résoudre dans $\mathbf{Z}$ le système

$$\begin{cases} x & \equiv & 7 & (\text{mod } 17) \\ x & \equiv & 8 & (\text{mod } 19) \end{cases}$$

2. L'entier 5 admet-il un inverse modulo 17 ? Si oui, le déterminer.

3. Résoudre dans $\mathbf{Z}$ le système

$$\begin{cases} 5x & \equiv & 1 & (\text{mod } 17) \\ x & \equiv & 8 & (\text{mod } 19) \end{cases}$$

4. Résoudre dans $\mathbf{Z}$ le système

$$\begin{cases} x & \equiv & 1 & (\text{mod } 21) \\ x & \equiv & 9 & (\text{mod } 28) \end{cases}$$

Éléments de solution 5

1. *Les entiers 17 et 19 sont premiers donc premiers entre eux (car distincts...). On peut donc utiliser le théorème des restes chinois.*
Cherchons d'abord deux entiers s et r tels $17s + 19r = 1$. On a $19 = 17 + 2$; $17 = 2 \times 8 + 1$. D'où $1 = 17 - 8 \times (19 - 17) = 9 - 8 \times 19$. Une solution est donc $s = 9$ et $r = -8$. D'après le théorème chinois, les solutions du système sont les entiers x tels que $x \equiv 9 \times 8 \times 17 - 8 \times 7 \times 19$ $(\text{mod } 17 \times 19) \equiv 1224 - 1064 \ (\text{mod } 323) \equiv 160 \ (\text{mod } 323)$.
2. *On peut remarquer que $7 \times 5 = 35 \equiv 1 \ (\text{mod } 17)$. Donc 5 admet 7 pour inverse modulo 14.*
Autre solution :
5 est premier avec 17 car ce sont deux nombres premiers distincts. L'entier 5 admet donc un inverse modulo 17. Cherchons x tel que $5x \equiv 1 \ (\text{mod } 17)$. Or $5x \equiv 1 \ (\text{mod } 17)$ est équivalent à l'existence d'un entier relatif k tel que $5x + 17k = 1$. L'algorithme d'Euclide donne $17 = 3 \times 5 + 2$; $5 = 2 \times 2 + 1$ donc $1 = 5 - 2 \times (17 - 3 \times 5) = 7 \times 5 - 2 \times 17$. Un inverse de 5 modulo 17 est donc 7.
3. *$5x \equiv 1 \ (\text{mod } 17)$ est équivalente à $7 \times 5x \equiv 7 \times 1 \ (\text{mod } 17)$ et donc à $x \equiv 7 \ (\text{mod } 17)$. Le système S_2 est donc équivalent au système S_1. Il a donc le même ensemble de solutions.*
4. *Montrons par l'absurde qu'il n'y a pas de solution. Soit donc a une solution.*
Modulo $\text{pgcd}(21, 28) = 7$, l'entier a vérifie

$$\begin{cases} a & \equiv & 1 & (\text{mod } 7) \\ a & \equiv & 9 & (\text{mod } 7) \equiv 2 \quad (\text{mod } 7) \end{cases}$$

ce qui est contradictoire.
Le système n'a donc pas de solution.
Autre solution :
$x \equiv 1 \ (\text{mod } 21)$ est équivalent à l'existence d'un entier relatif y tel que $x = 1 + 21y$. Reportons dans la deuxième équation du système et on obtient $1 + 21y \equiv 9 \ (\text{mod } 28)$ donc $21y \equiv 8 \ (\text{mod } 28)$. Il existe donc un entier relatif z tel que $21y = 8 + 28z$. Or 7 divise 21 et 28, donc divise $21y - 28z$, mais 7 ne divise pas 8. Le système S_3 n'a donc pas de solution.

Exercice 6

5 points

Le but de l'exercice est de montrer que l'ensemble X des nombres premiers congrus à 3 modulo 4, c'est-à-dire de la forme $4i + 3$ avec $i \in \mathbf{N}$, est infini.

1. Montrer que l'ensemble X est non vide.

2. Soit p un entier premier impair. Montrer que ($p \equiv 1 \ (\text{mod } 4)$ ou $p \equiv 3 \ (\text{mod } 4)$).

3. Soit n un entier naturel. Montrer que, si n est congru à 3 modulo 4, alors n admet un diviseur premier congru à 3 modulo 4. (*On pourra utiliser la décomposition en produits de facteurs premiers de n, puis un raisonnement par l'absurde.*)

4. Supposons que X est fini et s'écrit donc $X = \{p_1, p_2, \cdots, p_k\}$ et posons

$$a = 4p_1p_2\cdots p_k - 1 = 4\prod_{j=1}^{k} p_j - 1.$$

Montrer, à l'aide d'une question précédente, que a admet un diviseur premier dans la liste $\{p_1, p_2, \cdots, p_k\}$ et aboutir à une contradiction.
5. Conclure.

Éléments de solution 6

1. *X est non vide car $3 = 4 \times 0 + 3$ est un nombre premier.*
2. *Soit p un entier premier impair. Alors p n'est pas divisible par 2. Or, pour tout entier naturel n, n est congru à 0, 1, 2 ou 3 modulo 4. Donc $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$. Dans les deux autres cas, p serait divisible par 2, ce qui n'est pas possible.*
3. *Soit n un entier naturel. Supposons n congru à 3 modulo 4, alors $n \neq 0$ ou 1. Donc $n \geq 2$ et on peut utiliser sa décomposition en produit de facteurs premiers : $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec $p_1 < p_2 < \cdots < p_k$ des entiers premiers et α_i des entiers naturels non nuls.*
Supposons que n n'admette aucun un diviseur premier congru à 3 modulo 4. Alors, avec les notations précédentes, pour tout entier i compris entre 0 et k, $p_i \not\equiv 3 \pmod 4$ et donc $p_i \equiv 1 \pmod 4$ d'après la question 2.
On en déduit que $n \equiv 1 \pmod 4$. Absurde. Donc n admet au moins un diviseur premier congru à 3 modulo 4.
4. *Supposons que X est fini et s'écrit donc $X = \{p_1, p_2, \cdots, p_k\}$ et posons $a = 4p_1p_2\cdots p_k - 1$. Alors $a \equiv -1 \pmod 4 \equiv 3 \pmod 4$. D'après la question 3, a admet un diviseur premier congru à 3 modulo 4 donc un des éléments de X. Notons p_m cet élément. Or p_m divise $4p_1p_2\cdots p_k$, donc divise $4p_1p_2\cdots p_k - a = 1$. On en déduit que $p_m = 1$. Absurde car p_m est un nombre premier.*
5. *On a montré, en raisonnant par l'absurde, que l'ensemble X des nombres premiers congrus à 3 modulo 4, c'est-à-dire de la forme $4i + 3$ avec $i \in \mathbf{N}$, est infini.*