BURHAN

Arithmétique dans $\mathbb{Z}$: exercices, niveau examen

2ème Année Baccalauréat · Sciences Mathématiques · Mathématiques

Version en ligne : burhan.ma/2bac/sciences-mathematiques/mathematiques/arithmetique-dans-z/exercices/examen

Chapitre	Palier	Exercices
Arithmétique dans $\mathbb{Z}$	Niveau examen	5

Exercice 1 3,5 pts

Un premier p et l'entier $2^p + 3^p - 5$

Soit p un nombre premier tel que $p \geq 5$. On pose :

$$A_p = 2^p + 3^p - 5.$$

On rappelle que, si deux entiers a et b divisent un entier n et si $a \wedge b = 1$, alors $ab \mid n$. C'est une conséquence du théorème de Gauss.

1. 0,5 pts

Montre que $p \wedge 6 = 1$.

INDICE

Les seuls diviseurs positifs de p sont 1 et p. Il suffit donc de savoir si p divise 6.

CORRIGÉ

Diviseurs de p. Comme p est premier, ses seuls diviseurs positifs sont 1 et p. Le PGCD $p \wedge 6$, diviseur positif de p, vaut donc 1 ou p.

p ne divise pas 6. Les diviseurs positifs de 6 sont 1, 2, 3 et 6. Or $p \geq 5$, et $p \neq 6$ car 6 n'est pas premier. Donc $p \nmid 6$, et $p \wedge 6 \neq p$.

Conclusion. $p \wedge 6 = 1$. En particulier, $p \nmid 2$ et $p \nmid 3$.

2. 0,75 pts

Montre que $2^p \equiv 2\ [p]$ et que $3^p \equiv 3\ [p]$.

INDICE

Le petit théorème de Fermat s'applique à 2 puis à 3. Vérifie ses deux hypothèses grâce à la question 1, puis multiplie la congruence obtenue.

CORRIGÉ

Pour 2. L'entier p est premier et, d'après la question 1, $p \nmid 2$. Le petit théorème de Fermat donne :

$$2^{p-1} \equiv 1\ [p].$$

En multipliant par 2, on obtient $2^p \equiv 2\ [p]$.

Pour 3. De même, p est premier et $p \nmid 3$. Le petit théorème de Fermat donne $3^{p-1} \equiv 1\ [p]$, puis $3^p \equiv 3\ [p]$ en multipliant par 3.

Conclusion. $2^p \equiv 2\ [p]$ et $3^p \equiv 3\ [p]$.

3. 0,5 pts

Déduis-en que $p \mid A_p$.

INDICE

Les congruences modulo p s'additionnent membre à membre.

CORRIGÉ

La congruence modulo p est compatible avec l'addition. D'après la question 2 :

$$\begin{aligned} A_p &= 2^p + 3^p - 5 \\ &\equiv 2 + 3 - 5 \ [p] \\ &\equiv 0 \ [p]. \end{aligned}$$

Conclusion. $A_p \equiv 0 \ [p]$, c'est-à-dire $p \mid A_p$.

4. 0,25 pts

Montre que $2 \mid A_p$.

INDICE

Regarde la parité de chacun des trois termes.

CORRIGÉ

On examine la parité de chacun des trois termes :

- 2^p est pair, car $p \geq 1$;
- 3^p est impair, comme produit de facteurs impairs, et 5 est impair.

La différence $3^p - 5$ de deux impairs est paire. Donc $A_p = 2^p + (3^p - 5)$ est la somme de deux entiers pairs.

Conclusion. A_p est pair : $2 \mid A_p$.

5. 0,5 pts

Montre que $3 \mid A_p$.

INDICE

Modulo 3, remplace 2 par -1 et souviens-toi que p est impair.

CORRIGÉ

On travaille modulo 3. On a $3^p \equiv 0 \ [3]$ et $2 \equiv -1 \ [3]$, donc $2^p \equiv (-1)^p \ [3]$.

Or p est un premier différent de 2, donc impair : $(-1)^p = -1$. Par compatibilité avec l'addition :

$$\begin{aligned} A_p &\equiv -1 + 0 - 5 \ [3] \\ &\equiv -6 \ [3] \\ &\equiv 0 \ [3]. \end{aligned}$$

Conclusion. $3 \mid A_p$.

6. `0,5 pts`

Déduis-en que $6 \mid A_p$, puis que $6p \mid A_p$.

INDICE

Applique deux fois le rappel de l'énoncé. Quelle primalité relative as-tu établie à la question 1 ?

CORRIGÉ

Divisibilité par 6. D'après les questions 4 et 5, $2 \mid A_p$ et $3 \mid A_p$. De plus, $2 \wedge 3 = 1$. Le rappel de l'énoncé, conséquence du théorème de Gauss, donne $6 \mid A_p$.

Divisibilité par $6p$. D'après la question 3, $p \mid A_p$. D'après la question 1, $6 \wedge p = 1$. Le même rappel, appliqué à 6 et à p, donne $6p \mid A_p$.

Conclusion. $6 \mid A_p$, puis $6p \mid A_p$.

7. `0,5 pts`

Application. Déduis-en le reste de la division euclidienne de $2^{13} + 3^{13}$ par 78.

INDICE

Vérifie d'abord que 13 satisfait les hypothèses de l'énoncé. Écris ensuite 78 sous la forme $6p$.

CORRIGÉ

Hypothèses. L'entier 13 est premier et $13 \geq 5$. De plus, $78 = 6 \times 13$.

Divisibilité. D'après la question 6, appliquée à $p = 13$, on a $78 \mid A_{13}$. Il existe donc un entier k tel que $2^{13} + 3^{13} - 5 = 78k$, soit :

$$2^{13} + 3^{13} = 78k + 5.$$

Reste. On a $0 \leq 5 < 78$.

Conclusion. Par unicité de la division euclidienne, le reste cherché est 5.

Exercice 2 4 pts

Deux congruences, modulo 43 et modulo 18

On cherche les entiers relatifs n qui vérifient le système :

$$(S) : \quad \begin{cases} n \equiv 3 \ [43] \\ n \equiv 11 \ [18] \end{cases}$$

On rappelle que $n \equiv 3 \ [43]$ équivaut à l'existence d'un entier relatif x tel que $n = 43x + 3$.

1. 0,5 pts

Montre, à l'aide de l'algorithme d'Euclide, que $43 \wedge 18 = 1$.

INDICE

Divise 43 par 18, puis chaque diviseur par le reste obtenu, jusqu'à un reste nul.

CORRIGÉ

On effectue les divisions euclidiennes successives :

- $43 = 18 \times 2 + 7$, avec $0 \leq 7 < 18$;
- $18 = 7 \times 2 + 4$, avec $0 \leq 4 < 7$;
- $7 = 4 \times 1 + 3$, avec $0 \leq 3 < 4$;
- $4 = 3 \times 1 + 1$, avec $0 \leq 1 < 3$;
- $3 = 1 \times 3 + 0$.

Conclusion. Le dernier reste non nul est 1. D'après l'algorithme d'Euclide, $43 \wedge 18 = 1$.

2. `0,75 pts`

Déduis-en un couple (u, v) d'entiers relatifs tel que $43u + 18v = 1$.

INDICE

Isole chaque reste dans les divisions de la question 1. Remonte ensuite de 1 vers 43 et 18, sans développer trop tôt.

CORRIGÉ

Les restes isolés. D'après les divisions de la question 1 :

- $1 = 4 - 3$;
- $3 = 7 - 4$;
- $4 = 18 - 2 \times 7$;
- $7 = 43 - 2 \times 18$.

Remontée. On remplace successivement 3, puis 4, puis 7 :

$$\begin{aligned} 1 &= 4 - (7 - 4) \\ &= 2 \times 4 - 7 \\ &= 2(18 - 2 \times 7) - 7 \\ &= 2 \times 18 - 5 \times 7 \\ &= 2 \times 18 \\ &\quad - 5(43 - 2 \times 18) \\ &= 12 \times 18 - 5 \times 43. \end{aligned}$$

Vérification. $43 \times (-5) + 18 \times 12 = -215 + 216 = 1$.

Conclusion. Le couple $(u, v) = (-5, 12)$ convient : $43u + 18v = 1$.

3. 0,5 pts

Montre que n vérifie (S) si et seulement s'il existe deux entiers relatifs x et y tels que $n = 43x + 3$ et $43x - 18y = 8$.

INDICE

Traduis chaque congruence par une égalité, comme dans le rappel de l'énoncé. Égale ensuite les deux écritures de n.

CORRIGÉ

Traduction des congruences. D'après le rappel, $n \equiv 3\ [43]$ équivaut à l'existence d'un entier relatif x tel que $n = 43x + 3$. De même, $n \equiv 11\ [18]$ équivaut à l'existence d'un entier relatif y tel que $n = 18y + 11$.

Sens direct. Si n vérifie (S), on dispose de tels entiers x et y. Alors $43x + 3 = 18y + 11$, donc $43x - 18y = 8$.

Réciproque. Supposons $n = 43x + 3$ et $43x - 18y = 8$, avec x et y entiers relatifs. Alors $n \equiv 3\ [43]$. De plus :

$$\begin{aligned} n &= 18y + 8 + 3 \\ &= 18y + 11, \end{aligned}$$

donc $n \equiv 11\ [18]$.

Conclusion. n vérifie (S) si et seulement s'il existe deux entiers relatifs x et y tels que $n = 43x + 3$ et $43x - 18y = 8$.

4. 0,5 pts

Vérifie que le couple $(-40, -96)$ est une solution de l'équation (E) : $43x - 18y = 8$.

INDICE

Multiplie par 8 l'égalité de la question 2. Fais ensuite apparaître -18 devant la seconde inconnue.

CORRIGÉ

D'après la question 2, $43 \times (-5) + 18 \times 12 = 1$. On multiplie par 8, puis on écrit $18 \times 96 = -18 \times (-96)$:

$$\begin{aligned} 8 &= 43 \times (-40) \\ &\quad + 18 \times 96 \\ &= 43 \times (-40) \\ &\quad - 18 \times (-96). \end{aligned}$$

Contrôle. $43 \times (-40) = -1720$ et $18 \times 96 = 1728$, or $-1720 + 1728 = 8$.

Conclusion. Le couple $(x_0, y_0) = (-40, -96)$ est une solution de (E).

5. 1 pts

Résous l'équation (E) dans $\mathbb{Z}^2$.

INDICE

Soustrais l'égalité de la question 4 à l'équation (E), puis applique le théorème de Gauss. Son hypothèse vient de la question 1.

CORRIGÉ

Une égalité de produits. Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E). On lui soustrait membre à membre l'égalité $43 \times (-40) - 18 \times (-96) = 8$ de la question 4 :

$$43(x + 40) = 18(y + 96).$$

Théorème de Gauss. Donc $18 \mid 43(x + 40)$. Or $18 \wedge 43 = 1$ d'après la question 1. D'après le théorème de Gauss, $18 \mid x + 40$. Il existe donc $k \in \mathbb{Z}$ tel que $x = -40 + 18k$.

Valeur de y. En remplaçant, $43 \times 18k = 18(y + 96)$. Comme $18 \neq 0$, on obtient $y + 96 = 43k$, soit $y = -96 + 43k$.

Réciproque. Soit $k \in \mathbb{Z}$. On a :

$$\begin{aligned} &43(-40 + 18k) \\ &\quad - 18(-96 + 43k) \\ &= -1720 + 1728 \\ &= 8. \end{aligned}$$

Conclusion. Les solutions de (E) dans $\mathbb{Z}^2$ sont les couples $(-40 + 18k,\ -96 + 43k)$, avec $k \in \mathbb{Z}$.

6. 0,5 pts

Déduis-en que n vérifie (S) si et seulement si $n \equiv 605\ [774]$.

INDICE

Remplace x par l'expression de la question 5 dans $n = 43x + 3$. Ramène ensuite la constante entre 0 et 773 par une division euclidienne.

CORRIGÉ

Expression de n. D'après les questions 3 et 5, n vérifie (S) si et seulement s'il existe $k \in \mathbb{Z}$ tel que $n = 43(-40 + 18k) + 3$. Comme $43 \times 18 = 774$, cela s'écrit :

$$n = 774k - 1717.$$

Réduction de la constante. On a $-1717 = 774 \times (-3) + 605$, avec $0 \leq 605 < 774$. Donc :

$$n = 774(k - 3) + 605.$$

Quand k décrit $\mathbb{Z}$, l'entier $k - 3$ décrit aussi $\mathbb{Z}$.

Contrôle. $605 = 43 \times 14 + 3$ et $605 = 18 \times 33 + 11$.

Conclusion. n vérifie (S) si et seulement si $n \equiv 605\ [774]$.

7. `0,25 pts`

Détermine les entiers n compris entre 3000 et 4000 qui vérifient (S).

INDICE

Écris $n = 605 + 774m$ avec m entier relatif, puis encadre m.

CORRIGÉ

Soit n un entier qui vérifie (S). D'après la question 6, il existe $m \in \mathbb{Z}$ tel que $n = 605 + 774m$.

Encadrement. La condition $3000 \leq n \leq 4000$ équivaut à $2395 \leq 774m \leq 3395$.

Valeurs de m. Si $m \leq 3$, alors $774m \leq 2322 < 2395$. Si $m \geq 5$, alors $774m \geq 3870 > 3395$. Seul $m = 4$ peut convenir, et $774 \times 4 = 3096$ est bien compris entre 2395 et 3395.

Conclusion. Un seul entier entre 3000 et 4000 vérifie (S) : $n = 3701$.

Exercice 3 3,5 pts

Les diviseurs premiers de a² + a + 1

Soit a un entier naturel non nul. On pose $n = a^2 + a + 1$, et l'on considère un nombre premier p tel que $p \mid n$.

On rappelle que :

$$a^3 - 1 = (a-1)(a^2 + a + 1).$$

1. 0,25 pts

Vérifie que $n \times 1 + a \times (-a - 1) = 1$. Déduis-en que $a \wedge n = 1$.

INDICE

Développe le membre de gauche. Pour la conclusion, pense au théorème de Bézout.

CORRIGÉ

Vérification. On développe :

$$\begin{aligned} & n \times 1 + a(-a-1) \\ &= a^2 + a + 1 - a^2 - a \\ &= 1. \end{aligned}$$

PGCD. On a donc $au + nv = 1$ avec $u = -a - 1$ et $v = 1$, deux entiers relatifs. D'après le théorème de Bézout, $a \wedge n = 1$.

Conclusion. L'égalité demandée est vraie, et $a \wedge n = 1$.

2. 0,25 pts

Déduis-en que $p \nmid a$.

INDICE

Raisonne par l'absurde : un diviseur commun de deux entiers divise leur PGCD.

CORRIGÉ

Supposons par l'absurde que $p \mid a$. Comme $p \mid n$ par hypothèse, p est un diviseur commun de a et de n. Il divise donc leur PGCD $a \wedge n$, qui vaut 1 d'après la question 1.

C'est impossible, car $p \geq 2$.

Conclusion. $p \nmid a$.

3. 0,5 pts

Montre que $a^3 \equiv 1\ [p]$.

INDICE

Utilise l'égalité rappelée dans l'énoncé, avec l'hypothèse $p \mid n$.

CORRIGÉ

D'après le rappel de l'énoncé, $a^3 - 1 = (a-1)n$. Comme $p \mid n$, p divise le produit $(a-1)n$, donc $p \mid a^3 - 1$.

Conclusion. $a^3 \equiv 1\ [p]$.

4. 0,25 pts

Justifie que $a^{p-1} \equiv 1\ [p]$.

INDICE

Quel théorème donne cette congruence ? Cite ses deux hypothèses avant de l'appliquer.

CORRIGÉ

On vérifie les deux hypothèses du petit théorème de Fermat :

- l'entier p est premier ;
- $p \nmid a$, d'après la question 2.

Conclusion. D'après le petit théorème de Fermat, $a^{p-1} \equiv 1\ [p]$.

5. 0,5 pts

Dans les questions 5 et 6, on suppose que $p \equiv 2\ [3]$. Montre que $a \equiv 1\ [p]$.

INDICE

Divise $p-1$ par 3 et écris a^{p-1} à l'aide de a^3. Combine ensuite les questions 3 et 4.

CORRIGÉ

Division de $p-1$ par 3. Comme $p \equiv 2\ [3]$, on a $p - 1 \equiv 1\ [3]$. Le reste de la division euclidienne de $p-1$ par 3 est donc 1 : $p - 1 = 3q + 1$, avec $q \in \mathbb{N}$.

Calcul de a^{p-1}. D'après la question 3, $a^3 \equiv 1\ [p]$, donc $(a^3)^q \equiv 1\ [p]$. Ainsi :

$$\begin{aligned} a^{p-1} &= (a^3)^q \times a \\ &\equiv a\ [p]. \end{aligned}$$

Conclusion. D'après la question 4, $a^{p-1} \equiv 1\ [p]$. Donc $a \equiv 1\ [p]$.

6. 0,5 pts

Déduis-en que $p \mid 3$. Conclus que l'hypothèse $p \equiv 2\ [3]$ est impossible.

INDICE

Calcule n modulo p avec la question 5, puis souviens-toi que $p \mid n$.

CORRIGÉ

Calcul de n modulo p. D'après la question 5, $a \equiv 1\ [p]$. Par compatibilité avec l'addition et la multiplication :

$$\begin{aligned} n &= a^2 + a + 1 \\ &\equiv 1 + 1 + 1\ [p] \\ &\equiv 3\ [p]. \end{aligned}$$

p divise 3. Comme $p \mid n$, on a $n \equiv 0\ [p]$, donc $3 \equiv 0\ [p]$: $p \mid 3$. Le seul diviseur premier de 3 est 3, donc $p = 3$.

Contradiction. Or $3 \equiv 0\ [3]$, ce qui contredit $p \equiv 2\ [3]$.

Conclusion. On a $p \mid 3$, et l'hypothèse $p \equiv 2\ [3]$ est impossible.

7. 0,5 pts

Déduis-en que $p = 3$ ou $p \equiv 1\ [3]$.

INDICE

Écris la division euclidienne de p par 3 et examine les trois restes possibles un par un.

CORRIGÉ

La division euclidienne de p par 3 s'écrit $p = 3q + r$, avec $q \in \mathbb{N}$ et $0 \leq r < 3$. Trois cas sont possibles :

- si $r = 0$, alors $3 \mid p$; comme p est premier, $p = 3$;
- si $r = 1$, alors $p \equiv 1\ [3]$;
- si $r = 2$, alors $p \equiv 2\ [3]$, ce qui est impossible d'après la question 6.

Conclusion. $p = 3$ ou $p \equiv 1\ [3]$.

8. 0,75 pts

Application. Décompose $931 = 30^2 + 30 + 1$ en produit de facteurs premiers, et vérifie le résultat de la question 7.

Montre ensuite que, pour tout entier naturel non nul a, l'entier $a^2 + a + 1$ n'est divisible ni par 5, ni par 11.

INDICE

Teste les petits premiers sur 931. Pour la seconde partie, cherche le reste de 5 et de 11 dans la division par 3.

CORRIGÉ

Décomposition. On a $30^2 + 30 + 1 = 900 + 31 = 931$. Puis $931 = 7 \times 133$ et $133 = 7 \times 19$. Donc :

$$931 = 7^2 \times 19,$$

avec 7 et 19 premiers.

Vérification. On a $7 = 3 \times 2 + 1$ et $19 = 3 \times 6 + 1$, donc $7 \equiv 1\ [3]$ et $19 \equiv 1\ [3]$. C'est conforme à la question 7, appliquée à $a = 30$.

Cas de 5 et de 11. Soit a un entier naturel non nul. On a $5 = 3 \times 1 + 2$ et $11 = 3 \times 3 + 2$. Ainsi 5 et 11 sont des premiers différents de 3, congrus à 2 modulo 3. D'après la question 7, aucun d'eux ne divise $a^2 + a + 1$.

Conclusion. $931 = 7^2 \times 19$, et ni 5 ni 11 ne divise jamais $a^2 + a + 1$.

Exercice 4 3,5 pts

Les entiers dont le carré est congru à 1

Soit p un nombre premier tel que $p \geq 3$.

On rappelle que, si p est premier et si p ne divise pas un entier m, alors $p \wedge m = 1$.

On rappelle aussi le théorème de Gauss : si $c \mid ab$ et $c \wedge a = 1$, alors $c \mid b$.

1. 0,25 pts

Soit x un entier tel que $x^2 \equiv 1\ [p]$. Montre que p divise $(x-1)(x+1)$.

INDICE

Traduis la congruence par une divisibilité, puis factorise $x^2 - 1$.

CORRIGÉ

Par définition de la congruence, $x^2 \equiv 1\ [p]$ signifie que $p \mid x^2 - 1$. Or :

$$x^2 - 1 = (x-1)(x+1).$$

Conclusion. p divise $(x-1)(x+1)$.

2. 0,75 pts

Déduis-en que $x \equiv 1\ [p]$ ou $x \equiv -1\ [p]$.

INDICE

Distingue deux cas, selon que p divise $x - 1$ ou non. Dans le second cas, utilise les deux rappels de l'énoncé.

CORRIGÉ

On distingue deux cas.

Premier cas : $p \mid x - 1$**.** Alors $x \equiv 1\ [p]$.

Second cas : $p \nmid x - 1$**.** Comme p est premier, le premier rappel donne $p \wedge (x-1) = 1$. Or $p \mid (x-1)(x+1)$ d'après la question 1. D'après le théorème de Gauss, $p \mid x + 1$, c'est-à-dire $x \equiv -1\ [p]$.

Conclusion. Dans les deux cas, $x \equiv 1\ [p]$ ou $x \equiv -1\ [p]$.

3. 0,5 pts

Montre la réciproque : si $x \equiv 1\ [p]$ ou $x \equiv -1\ [p]$, alors $x^2 \equiv 1\ [p]$. Montre ensuite que 1 et -1 ne sont pas congrus modulo p.

INDICE

Élève chaque congruence au carré. Pour la seconde partie, calcule $1-(-1)$ et utilise $p \geq 3$.

CORRIGÉ

Réciproque. Si $x \equiv 1\ [p]$, alors $x^2 \equiv 1^2\ [p]$, soit $x^2 \equiv 1\ [p]$. Si $x \equiv -1\ [p]$, alors $x^2 \equiv (-1)^2\ [p]$, soit encore $x^2 \equiv 1\ [p]$.

1 et -1 ne sont pas congrus. On a $1-(-1)=2$. Comme $p \geq 3$, on a $0<2<p$. Un multiple non nul de p est, en valeur absolue, au moins égal à p. Donc $p \nmid 2$.

Conclusion. Les solutions de $x^2 \equiv 1\ [p]$ sont exactement les entiers congrus à 1 ou à -1 modulo p, et ces deux cas sont distincts.

4. 0,5 pts

Soit a un entier tel que $p \nmid a$. Montre que $a \times a^{p-2} \equiv 1\ [p]$: l'entier a^{p-2} est un inverse de a modulo p.

INDICE

Vérifie que $p-2 \geq 1$, puis applique le petit théorème de Fermat en citant ses deux hypothèses.

CORRIGÉ

L'exposant. Comme $p \geq 3$, on a $p-2 \geq 1$: a^{p-2} est un entier.

Petit théorème de Fermat. L'entier p est premier et $p \nmid a$. D'après le petit théorème de Fermat, $a^{p-1} \equiv 1\ [p]$.

Conclusion. Comme $a \times a^{p-2} = a^{p-1}$, on a $a \times a^{p-2} \equiv 1\ [p]$: l'entier a^{p-2} est un inverse de a modulo p.

5. 0,5 pts

Avec l'entier a de la question 4, montre que $a^{p-2} \equiv a\ [p]$ si et seulement si $a \equiv 1\ [p]$ ou $a \equiv -1\ [p]$.

INDICE

Dans un sens, multiplie par a et utilise la question 4. Dans l'autre, remarque que $p-2$ est impair.

CORRIGÉ

Sens direct. Supposons $a^{p-2} \equiv a\ [p]$. En multipliant par a, on obtient $a \times a^{p-2} \equiv a^2\ [p]$. D'après la question 4, le membre de gauche est congru à 1 : $a^2 \equiv 1\ [p]$. D'après la question 2, $a \equiv 1\ [p]$ ou $a \equiv -1\ [p]$.

Réciproque, si $a \equiv 1\ [p]$. Alors $a^{p-2} \equiv 1^{p-2}\ [p]$, soit $a^{p-2} \equiv 1\ [p]$. Donc $a^{p-2} \equiv a\ [p]$.

Réciproque, si $a \equiv -1\ [p]$. Alors $a^{p-2} \equiv (-1)^{p-2}\ [p]$. Or p est un premier différent de 2, donc impair, et $p-2$ est impair. Ainsi $(-1)^{p-2} = -1$, et $a^{p-2} \equiv a\ [p]$.

Conclusion. $a^{p-2} \equiv a\ [p]$ si et seulement si $a \equiv 1\ [p]$ ou $a \equiv -1\ [p]$.

6. `0,5 pts`

Application. Décompose 253 en produit de facteurs premiers.

Montre que, pour tout entier x : $x^2 \equiv 1\ [253]$ si et seulement si $x^2 \equiv 1\ [11]$ et $x^2 \equiv 1\ [23]$.

INDICE

Teste les premiers 2, 3, 5, 7 et 11. Pour la réciproque, pense à la conséquence du théorème de Gauss sur deux diviseurs premiers entre eux.

CORRIGÉ

Décomposition. On teste les premiers 2, 3, 5 et 7 :

- $253 = 2 \times 126 + 1$;
- $253 = 3 \times 84 + 1$;
- $253 = 5 \times 50 + 3$;
- $253 = 7 \times 36 + 1$.

Aucun ne divise 253. Puis $253 = 11 \times 23$. Les entiers 11 et 23 sont premiers : ni 2 ni 3 ne les divisent, et $5^2 = 25 > 23$. La décomposition cherchée est donc $253 = 11 \times 23$.

Soit x un entier.

Sens direct. Si $253 \mid x^2 - 1$, alors 11 et 23, qui divisent 253, divisent aussi $x^2 - 1$.

Réciproque. Supposons que 11 et 23 divisent $x^2 - 1$. Ce sont deux premiers distincts, donc $11 \wedge 23 = 1$. D'après la conséquence du théorème de Gauss, leur produit 253 divise $x^2 - 1$.

Conclusion. $253 = 11 \times 23$ et, pour tout entier x : $x^2 \equiv 1\ [253]$ si et seulement si $x^2 \equiv 1\ [11]$ et $x^2 \equiv 1\ [23]$.

7. `0,5 pts`

Déduis-en que l'équation $x^2 \equiv 1\ [253]$ a exactement quatre solutions x telles que $0 \leq x \leq 252$. Vérifie que 45 et 208 en font partie.

INDICE

Modulo 11 comme modulo 23, l'entier x est congru à 1 ou à -1 : cela fait quatre cas. Montre que chaque cas a au plus une solution entre 0 et 252.

CORRIGÉ

Quatre cas. Soit x un entier. D'après la question 6, puis les questions 2 et 3 appliquées à $p = 11$ et à $p = 23$, $x^2 \equiv 1\ [253]$ équivaut à :

- $x \equiv 1\ [11]$ ou $x \equiv -1\ [11]$;
- et $x \equiv 1\ [23]$ ou $x \equiv -1\ [23]$.

Cela fait quatre cas.

Au plus une solution par cas. Soient x et x' deux solutions entre 0 et 252, dans le même cas. Alors $11 \mid x - x'$ et $23 \mid x - x'$, donc $253 \mid x - x'$, comme à la question 6. Or $-252 \leq x - x' \leq 252$, donc $x - x' = 0$.

Une solution par cas.

x	division par 11	division par 23
1	$x \equiv 1\ [11]$	$x \equiv 1\ [23]$
45	$45 = 11 \times 4 + 1$	$45 = 23 \times 1 + 22$, donc $45 \equiv -1\ [23]$
208	$208 = 11 \times 18 + 10$, donc $208 \equiv -1\ [11]$	$208 = 23 \times 9 + 1$
252	$252 = 11 \times 22 + 10$, donc $252 \equiv -1\ [11]$	$252 = 23 \times 10 + 22$, donc $252 \equiv -1\ [23]$

Contrôle. $45^2 = 2025 = 253 \times 8 + 1$.

Conclusion. Il y a exactement quatre solutions entre 0 et 252 : 1, 45, 208 et 252. En particulier, 45 et 208 en font partie.

Exercice 5 3,5 pts

La somme et le PPCM de deux entiers

Soient a et b deux entiers naturels non nuls. On note $d = a \wedge b$ et $m = a \vee b$. Comme d divise a et b, on écrit $a = da_1$ et $b = db_1$, où a_1 et b_1 sont des entiers naturels non nuls.

On rappelle que $(a \wedge b)(a \vee b) = ab$.

On rappelle aussi l'identité de Bézout : il existe deux entiers relatifs u et v tels que $au + bv = a \wedge b$.

1. 0,5 pts

Montre que $a_1 \wedge b_1 = 1$, puis que $m = da_1b_1$.

INDICE

Divise par d l'égalité de Bézout du rappel. Pour m, utilise le premier rappel.

CORRIGÉ

PGCD de a_1 et b_1. D'après l'identité de Bézout, il existe deux entiers relatifs u et v tels que $au + bv = d$, soit $da_1u + db_1v = d$. Comme $d \neq 0$, on peut diviser par d :

$$a_1u + b_1v = 1.$$

D'après le théorème de Bézout, $a_1 \wedge b_1 = 1$.

Expression de m. D'après le premier rappel, $dm = ab = d^2a_1b_1$. Comme $d \neq 0$, on obtient $m = da_1b_1$.

Conclusion. $a_1 \wedge b_1 = 1$ et $m = da_1b_1$.

2. 0,75 pts

Montre que $(a_1 + b_1) \wedge a_1b_1 = 1$.

INDICE

Raisonne par l'absurde avec un diviseur premier de ce PGCD. Un premier qui divise a_1b_1 divise a_1 ou b_1 .

CORRIGÉ

Un diviseur premier. On pose $c = (a_1 + b_1) \wedge a_1b_1$, et on suppose par l'absurde que $c \geq 2$. Alors c admet au moins un diviseur premier p. Ce premier divise $a_1 + b_1$ et a_1b_1.

p divise a_1 ou b_1. Comme p est premier et $p \mid a_1b_1$, la conséquence du théorème de Gauss donne $p \mid a_1$ ou $p \mid b_1$:

- si $p \mid a_1$, alors p divise $(a_1 + b_1) - a_1 = b_1$;
- si $p \mid b_1$, alors p divise $(a_1 + b_1) - b_1 = a_1$.

Contradiction. Dans les deux cas, p divise a_1 et b_1, donc $p \mid a_1 \wedge b_1$. Or $a_1 \wedge b_1 = 1$ d'après la question 1, et $p \geq 2$: c'est impossible.

Conclusion. $c = 1$, c'est-à-dire $(a_1 + b_1) \wedge a_1b_1 = 1$.

3. 0,5 pts

Déduis-en que $(a+b)\wedge m = d$, puis que $a_1+b_1 = \dfrac{a+b}{d}$ et $a_1 b_1 = \dfrac{m}{d}$.

INDICE

Écris une égalité de Bézout pour a_1+b_1 et $a_1 b_1$, puis multiplie-la par d.

CORRIGÉ

Une égalité de Bézout. D'après la question 2 et le théorème de Bézout, il existe deux entiers relatifs u et v tels que :

$$(a_1+b_1)u + a_1 b_1 v = 1.$$

On multiplie par d. Comme $a+b = d(a_1+b_1)$ et $m = d a_1 b_1$ (question 1), on obtient :

$$(a+b)u + mv = d.$$

PGCD de $a+b$ et m. Tout diviseur commun positif de $a+b$ et de m divise donc d, et lui est inférieur ou égal. Or d divise $a+b = d(a_1+b_1)$ et $m = d a_1 b_1$. Ainsi d est le plus grand diviseur commun positif de $a+b$ et de m.

Quotients. Les égalités $a+b = d(a_1+b_1)$ et $m = d a_1 b_1$, avec $d \neq 0$, donnent $a_1+b_1 = \dfrac{a+b}{d}$ et $a_1 b_1 = \dfrac{m}{d}$.

Conclusion. $(a+b)\wedge m = d$, $a_1+b_1 = \dfrac{a+b}{d}$ et $a_1 b_1 = \dfrac{m}{d}$.

4. 0,25 pts

Application. On cherche les couples (a,b) d'entiers naturels non nuls tels que $a+b = 96$ et $a \vee b = 180$.

Calcule $96 \wedge 180$ par l'algorithme d'Euclide.

INDICE

Divise 180 par 96, puis chaque diviseur par le reste obtenu.

CORRIGÉ

On effectue les divisions euclidiennes successives :

- $180 = 96 \times 1 + 84$, avec $0 \leq 84 < 96$;
- $96 = 84 \times 1 + 12$, avec $0 \leq 12 < 84$;
- $84 = 12 \times 7 + 0$.

Conclusion. Le dernier reste non nul est 12. D'après l'algorithme d'Euclide, $96 \wedge 180 = 12$.

5. 0,5 pts

Déduis-en tous les couples (a, b) cherchés à la question 4.

INDICE

Avec la question 3, calcule d, $a_1 + b_1$ et $a_1 b_1$. Cherche ensuite a_1 parmi les diviseurs positifs de $a_1 b_1$, sans oublier la réciproque.

CORRIGÉ

Valeurs de d, $a_1 + b_1$ et $a_1 b_1$. Soit (a, b) un tel couple. D'après les questions 3 et 4 :

$$\begin{aligned} d &= (a + b) \wedge m \\ &= 96 \wedge 180 \\ &= 12. \end{aligned}$$

Comme $96 = 12 \times 8$ et $180 = 12 \times 15$, la question 3 donne $a_1 + b_1 = 8$ et $a_1 b_1 = 15$.

Recherche de a_1. L'entier a_1 est un diviseur positif de 15 : 1, 3, 5 ou 15.

- Pour $a_1 = 1$ ou $a_1 = 15$, la somme $a_1 + b_1$ vaut $1 + 15 = 16 \neq 8$.
- Pour $a_1 = 3$, on a $b_1 = 5$; pour $a_1 = 5$, on a $b_1 = 3$. La somme vaut bien 8.

Avec $a = 12a_1$ et $b = 12b_1$: $(a, b) = (36, 60)$ ou $(a, b) = (60, 36)$.

Réciproque. On a $36 + 60 = 96$. Par l'algorithme d'Euclide, $60 = 36 \times 1 + 24$, $36 = 24 \times 1 + 12$ et $24 = 12 \times 2 + 0$, donc $36 \wedge 60 = 12$. D'après le premier rappel, $12 \times (36 \vee 60) = 36 \times 60$. Or $36 \times 60 = 2160 = 12 \times 180$, donc $36 \vee 60 = 180$.

Conclusion. Les couples cherchés sont $(36, 60)$ et $(60, 36)$.

6. 0,5 pts

Montre qu'il n'existe aucun couple (a, b) d'entiers naturels non nuls tels que $a + b = 100$ et $a \vee b = 150$.

INDICE

Procède comme aux questions 4 et 5, puis compare les valeurs obtenues pour $a_1 + b_1$ et pour $a_1 b_1$.

CORRIGÉ

Supposons par l'absurde qu'un tel couple (a, b) existe.

PGCD. Par l'algorithme d'Euclide, $150 = 100 \times 1 + 50$ et $100 = 50 \times 2 + 0$, donc $100 \wedge 150 = 50$. D'après la question 3, $d = 50$.

Somme et produit. Comme $100 = 50 \times 2$ et $150 = 50 \times 3$, on a $a_1 + b_1 = 2$ et $a_1 b_1 = 3$.

Contradiction. Les entiers naturels non nuls a_1 et b_1 ont pour somme 2, donc $a_1 = b_1 = 1$. Mais alors $a_1 b_1 = 1 \neq 3$.

Conclusion. Aucun couple ne convient : une somme égale à 100 et un PPCM égal à 150 sont incompatibles.

7. 0,5 pts

Soit p un nombre premier. Détermine les couples (a, b) d'entiers naturels non nuls tels que $a + b = p(p+1)$ et $a \vee b = p^2$.

INDICE

Un diviseur commun à $p(p+1)$ et à p^2 divise leur différence. Les diviseurs positifs de p sont 1 et p.

CORRIGÉ

Soit (a, b) un tel couple.

PGCD. Un diviseur commun à $p(p+1)$ et à p^2 divise leur différence :

$$p(p+1) - p^2 = p.$$

Inversement, p divise ces deux entiers. Donc $p(p+1) \wedge p^2 = p$.

Somme et produit. D'après la question 3, $d = p$, puis $a_1 + b_1 = p + 1$ et $a_1 b_1 = p$.

Valeurs de a_1 et b_1. L'entier a_1 est un diviseur positif du premier p :

- soit $a_1 = 1$ et $b_1 = p$;
- soit $a_1 = p$ et $b_1 = 1$.

Dans les deux cas, $a_1 + b_1 = p + 1$. Donc $(a, b) = (p, p^2)$ ou $(a, b) = (p^2, p)$.

Réciproque. On a $p + p^2 = p(p+1)$. Comme p divise p^2, on a $p \wedge p^2 = p$. D'après le premier rappel, $p \times (p \vee p^2) = p \times p^2$, donc $p \vee p^2 = p^2$.

Conclusion. Les couples cherchés sont (p, p^2) et (p^2, p).