DOMAINE : Arithmétique
NIVEAU : Intermédiaire
CONTENU : Exercices

AUTEUR : Noé DE RANCOURT
STAGE : Cachan 2011 (junior)

Exercices d'arithmétique

- Énoncés -

Exercice 1

a) Trouver tous les entiers $n \in \mathbb{N}^*$ qui possèdent un nombre impair de diviseurs (positifs).

b) Soit $n \in \mathbb{N}^*$. On note d le nombre de diviseurs de n, et D le produit de ses diviseurs. Montrer que $n^d = D^2$.

c) On suppose que la décomposition en facteurs premiers de n s'écrit $p_1^{\alpha_1} ... p_r^{\alpha_r}$. Exprimer le nombre de diviseurs de n en fonction des α_i.

Exercice 2 Montrer que pour tout $n \in \mathbb{N}$, la fraction $\dfrac{21n+4}{14n+3}$ est irréductible.

Exercice 3

a) Soit a un entier supérieur ou égal à 2, et m, $n \in \mathbb{N}$. Montrer que si $m \mid n$, alors $(a^m - 1) \mid (a^n - 1)$.

b) On suppose toujours que $m \mid n$. A quelle condition a-t-on $(a^m + 1) \mid (a^n + 1)$? Que peut-on dire dans le cas contraire ?

Exercice 4

a) Montrer que pour tout $a \in \mathbb{N}$, l'équation $x^2 + y^2 + z^2 = 8a + 7$ n'a pas de solutions dans $\mathbb{Q}^3$.

b) Trouver tous les entiers naturels n tels que $7^n + 8$ soit un carré parfait.

Exercice 5 Soit p un nombre premier. Montrer que si $a \equiv b \mod p$, alors $a^p \equiv b^p \mod p^2$.

Exercice 6 Les systèmes suivants admettent-ils des solutions ?

a) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 6 \mod 14 \end{cases}$

b) $\begin{cases} x \equiv 5 \mod 12 \\ x \equiv 7 \mod 15 \end{cases}$

c) $\begin{cases} x \equiv 10 \mod 12 \\ x \equiv 16 \mod 21 \end{cases}$

Exercice 7 Soit P un polynôme à coefficients entiers. Montrer que pour tous entiers a et b, $(b-a) \mid (P(b)-P(a))$.

Exercice 8 Résoudre dans $\mathbb{Q}$ l'équation $5x^3+3x^2+3x-2=0$.

Exercice 9

a) Soit p un nombre premier congru à 3 modulo 4, et a et b deux entiers tels que $p \mid (a^2+b^2)$. Montrer que $p \mid a$ et $p \mid b$.

b) En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Exercice 10 (Théorème de Wilson) Soit p un entier supérieur ou égal à 2. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \mod p$.

Exercice 11 Soit p un nombre premier. Montrer qu'il existe des entiers x et y tels que x^2+y^2+2 soit divisible par p.

Exercice 12 On définit la suite (u_n) par $u_0 = u_1 = 0$ et la relation de récurrence $u_{n+2} = u_{n+1} + u_n + 1$ pour tout $n \geqslant 0$. Montrer qu'il existe un entier $n \geqslant 1$ tel que u_n et u_{n+1} soient divisibles par 2011^{2012}.

- Corrigés -

Solution de l'exercice 1

a) Le point important est de remarquer que si d est un diviseur de n, alors $\frac{n}{d}$ aussi. (En fait, la fonction $f : d \mapsto \frac{n}{d}$ de l'ensemble des diviseurs de n dans lui même est une *involution*, c'est-à-dire que pour tout d, $f(f(d)) = d$). Si pour tout diviseur d de n, on a $d \neq \frac{n}{d}$, alors on peut partitionner l'ensemble des diviseurs de n en paires $\left\{d, \frac{n}{d}\right\}$, et cet ensemble est donc de cardinal pair. Sinon, il existe un diviseur d_0 de n tel que $\frac{n}{d_0} = d_0$, c'est-à-dire $n = d_0^2$, et n est un carré parfait. Dans ce cas, on peut partitionner

l'ensemble des diviseurs de n en un certain nombre de paires $\left\{d, \frac{n}{d}\right\}$ et un singleton $\{d_0\}$, et cet ensemble est donc de cardinal impair. Les $n \in \mathbb{N}^*$ qui possèdent un nombre impair de diviseurs sont donc exactement les carrés parfaits.

b) On utilise encore la remarque de la question précédente. Si l'ensemble des diviseurs de n est $\{x_1, ..., x_d\}$, alors on peut réécrire cet ensemble $\left\{\frac{n}{x_1}, ..., \frac{n}{x_d}\right\}$. Donc $D = x_1 \cdot ... \cdot x_d = \frac{n}{x_1} \cdot ... \cdot \frac{n}{x_d}$, d'où $D^2 = \left(x_1 \frac{n}{x_1}\right) \cdot ... \cdot \left(x_d \frac{n}{x_d}\right) = n^d$.

c) On remarque qu'un entier naturel divise n si et seulement si il s'écrit $p_1^{\beta_1} ... p_r^{\beta_r}$, avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout i. Le nombre de diviseurs de n est donc égal au nombre de choix possibles de la suite des β_i vérifiant ces conditions. i étant fixé, on a $\alpha_i + 1$ choix possibles pour la valeur de β_i. On a donc $(\alpha_1 + 1)...(\alpha_r + 1)$ choix possibles pour toute la suite, et c'est le nombre de diviseurs de n.

Solution de l'exercice 2 On rappelle que la fraction $\frac{a}{b}$ est irréductible si et seulement si a et b sont premiers entre eux. Ici, on a $3 \cdot (14n + 3) - 2 \cdot (21n + 4) = 1$ pour tout n, donc par le théorème de Bézout, $14n + 3$ et $21n + 4$ sont premiers entre eux. La fraction $\frac{21n + 4}{14n + 3}$ est donc irréductible.

Solution de l'exercice 3

a) Remarquons que quitte à poser $b = a^m$ et $d = \frac{n}{m}$, on est ramené à montrer que $(b - 1) \mid (b^d - 1)$. On peut alors utiliser l'identité $(b^d - 1) = (b - 1)(b^{d-1} + b^{d-2} + ... + b + 1)$, qui donne immédiatement le résultat. On peut aussi travailler modulo $b - 1$: comme $b \equiv 1 \mod b - 1$, on en déduit que $b^d \equiv 1 \mod b - 1$, d'où le résultat.

b) On cherche cette fois à quelle condition $(b + 1) \mid (b^d + 1)$. On va montrer que c'est vrai lorsque d est impair. L'identité $b^d + 1 = (b + 1)(b^{d-1} - bd - 2 + ... - b + 1)$ (vraie uniquement lorsque d est impair) le montre immédiatement. On retrouve ce résultat en regardant modulo $b + 1$: comme $b \equiv -1 \mod b + 1$, alors $b^d \equiv (-1)^d \equiv -1 \mod b + 1$. Si, par contre, d est pair, on a $b^d \equiv (-1)^d \equiv 1 \mod b + 1$, donc $(b + 1) \mid (b^d - 1)$.
Conclusion : si $\frac{n}{m}$ est impair, alors $(a^m + 1) \mid (a^n + 1)$, et sinon, $(a^m + 1) \mid (a^n - 1)$.

Solution de l'exercice 4

a) Pour se ramener à une équation à inconnues entières, on pose $x = \frac{X}{T}$, $y = \frac{Y}{T}$ et $z = \frac{Z}{T}$, où $X, Y, Z \in \mathbb{Z}$, et où $T \in \mathbb{N}^*$ est l'entier minimal permettant cette écriture (autrement dit, T est le PPCM des dénominateurs de x, y, et z écrits sous forme irréductible). On a alors $X^2 + Y^2 + Z^2 = (8a+7)T^2$. Motivés par la présence de carrés, on regarde modulo 8 (auquel un carré peut être congru à 0, 1 ou 4 uniquement). L'équation devient alors $X^2 + Y^2 + Z^2 + T^2 \equiv 0 \mod 8$.
Or, au moins un des entiers X, Y, Z et T est impair, sinon on pourrait les remplacer respectivement par $\frac{X}{2}$, $\frac{Y}{2}$, $\frac{Z}{2}$ et $\frac{T}{2}$, ce qui contredirait la minimalité de T. Sans perte de généralité, on peut supposer que c'est X. On a alors $X^2 \equiv 1 \mod 8$, d'où $1 + Y^2 + Z^2 + T^2 \equiv 0 \mod 8$. En regardant les valeurs pouvant être prises modulo 8 par X^2, Y^2 et Z^2, on voit que cette égalité ne peut pas être vérifiée.

b) On doit résoudre l'équation diophantienne $7^n + 8 = x^2$ (dans laquelle on peut considérer, sans perte de généralité, que $x \geqslant 0$). La présence du carré nous incite à regarder modulo 4. x^2 peut être congru à 0 ou à 1, et $7^n \equiv (-1)^n \equiv \pm 1 \mod 4$. On a donc forcément $7^n \equiv (-1)^n \equiv 1 \mod 4$, donc n est pair ; on peut écrire $n = 2m$, avec $m \in \mathbb{N}^*$. On a alors $8 = x^2 - (7^m)^2 = (x - 7^m)(x + 7^m)$, donc $x + 7^m \leqslant 8$ et à fortiori, $7^m \leqslant 8$. Donc $m = 0$ ou 1, et on vérifie réciproquement que $m = 0$ est la seule solution. Le seul entier n tel que $7^n + 8$ soit un carré parfait est donc 0.

Solution de l'exercice 5 Comme $a \equiv b \mod p$, alors il existe un entier k tel que $b = a + kp$. On utilise alors la formule du binôme :

$$b^p - a^p = (a + kp)^p - a^p = \sum_{i=1}^{p} \binom{p}{i} (kp)^i a^{p-i}$$

Or, pour tout i tel que $1 \leqslant i \leqslant p-1$, on a $p! = i!(p-i)!\binom{p}{i}$, et p divise $p!$ mais ne divise ni $i!$, ni $(p-i)!$, donc par le théorème de Gauss, $p \mid \binom{p}{i}$. Pour $1 \leqslant i \leqslant p-1$, on a donc $p^2 \mid \binom{p}{i}(kp)^i a^{p-i}$, ceci restant vrai pour $i = p$. Donc $p^2 \mid (b^p - a^p)$, d'où le résultat.

Solution de l'exercice 6

a) 3 étant premier avec 14, d'après le théorème chinois, le système admet des solutions.

b) La congruence $x \equiv 5 \mod 12$ implique $x \equiv 2 \mod 3$, et $x \equiv 7 \mod 15$ implique $x \equiv 1 \mod 3$. Ces deux congruences sont incompatibles, donc le système n'admet pas de solutions.

c) La congruence $x \equiv 10 \mod 12$ implique $x \equiv 1 \mod 3$ et $x \equiv 2 \mod 4$. Or, 3 et 4 étant premiers entre eux, le théorème chinois nous dit que le système de congruences :

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 4 \end{cases}$$

est équivalent à une unique congruence modulo 12, c'est donc forcément $x \equiv 10 \mod 12$.

De la même façon, on montre que la congruence $x \equiv 16 \mod 21$ est équivalente au système

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 7 \end{cases}$$

Le système initial est donc équivalent au système

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 4 \\ x \equiv 2 \mod 7 \end{cases}$$

qui par le théorème chinois admet des solutions.

Solution de l'exercice 7 On regarde modulo $n = b - a$. On a $a \equiv b \mod n$, et comme la relation de congruence est compatible avec l'addition et la multiplication, ceci implique que $P(a) \equiv P(b) \mod n$, donc $n \mid (P(b) - P(a))$.

Solution de l'exercice 8 Considérons une solution rationnelle éventuelle $\frac{p}{q}$ (écrite sous forme irréductible) de l'équation. On a alors

$$5\left(\frac{p}{q}\right)^3 + 3\left(\frac{p}{q}\right)^2 + 3\frac{p}{q} - 2 = 0$$

donc $5p^3 + 3p^2q + 3pq^2 - 2q^3 = 0$.

On a donc $5p^3 = q(-3p^2 - 3pq + 2q^2)$, donc $q \mid 5p^3$, et comme q est premier avec p (donc avec p^3), on en déduit par Gauss que $q \mid 5$. Par une méthode tout à fait analogue, on montre que $p \mid 2$. Les seules solutions rationnelles possibles de l'équation sont donc ± 1, ± 2, $\pm\frac{1}{5}$, et $\pm\frac{2}{5}$. On n'a plus qu'à vérifier, à la main, si chacune des solutions potentielles est réellement solution ou non, et on voit que la seule solution est $\frac{2}{5}$.

Remarque : Cette méthode fournit un moyen de résoudre dans $\mathbb{Q}$ n'importe quelle équation polynômiale à coefficients entiers (et donc à coefficients rationnels, puisqu'on peut se ramener à une équation à coefficients entiers quitte à multiplier par une bonne constante).

Solution de l'exercice 9

a) La condition $p \mid (a^2 + b^2)$ se réécrit $b^2 \equiv -a^2 \mod p$. Raisonnons par l'absurde et supposons que a ne soit pas divisible par p. a admet alors un inverse a^{-1} modulo p (i.e. un entier tel que $aa^{-1} \equiv 1 \mod p$), et on a $(ba^{-1})^2 \equiv -1 \mod p$. -1 est donc un carré modulo p.
Par le critére d'Euler, cela implique que $(-1)^{\frac{p-1}{2}} \equiv 1 \mod p$, donc que $\frac{p-1}{2}$ est pair. On en déduit que $p \equiv 1 \mod 4$, ce qui est contraire à notre hypothèse. Donc $p \mid a$, et par la même occasion, $p \mid b$.

b) On va faire un démonstration analogue à celle d'Euclide pour montrer que l'ensemble des nombres premiers est infini. Par l'absurde, supposons que l'ensemble des nombres premiers congrus à 1 modulo 4 soit fini, et notons ses éléments $p_1, ..., p_n$. On pose $M = (2p_1...p_n)^2 + 1$. M n'est clairement divisible par aucun des p_i, ni par 2, donc tous ses diviseur premiers sont congrus à 3 modulo 4. Notons p un tel diviseur ; alors en appliquant la première question à p avec $a = 2p_1...p_n$ et $b = 1$, on en déduit que $p \mid 1$, ce qui est absurde. Donc l'ensemble des nombres premiers congrus à 1 modulo 4 est infini.

Solution de l'exercice 10 Le point clé de cette preuve est le fait que tout entier premier avec p admet un inverse modulo p ; en particulier, si p est premier, c'est le cas de tout entier non nul modulo p. De plus, l'inversion est involutive, c'est-à- dire que $(a^{-1})^{-1} \equiv a \mod p$ pour tout a.

Si p n'est pas premier, l'un des facteurs du produit $(p-1)!$ est un diviseur de p, donc est non inversible modulo p. Donc $(p-1)!$ n'est pas inversible modulo p, et n'est donc pas congru à -1, qui, lui, est inversible.

Réciproquement, si p est premier, alors on va partitionner l'ensemble $\{1, ..., p-1\}$ en paires d'entiers deux à deux inverses modulo p. Pour cela, il faut connaître les entiers x qui sont leur propre inverse ; ceux-là sont solutions de l'équation $x^2 \equiv 1 \mod p$, de degré 2, donc qui admet au plus deux solutions : ce sont donc 1 et -1 (ce dernier étant congru à $p-1$ modulo p). On regroupe les autres par paires d'inverses $\left\{x_i, x_i^{-1}\right\}$, de sorte que $\{1\}$, $\{p-1\}$ et les $\left\{x_i, x_i^{-1}\right\}$ forment une partition de $\{1, ..., p-1\}$.

En réorganisant l'ordre des facteurs du produit, on a alors

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (x_1 x_1^{-1}) \cdot ... \cdot (x_r x_r^{-1}) \equiv p-1 \equiv -1 \mod p$$

Solution de l'exercice 11 L'idée est de montrer que les ensembles des valeurs prises modulo p par x^2 et par $-2-y^2$ sont suffisamment gros, donc s'intersectent. Il faut donc calculer leur cardinal.

Si $p = 2$, le résultat est trivial. Sinon, considérons l'ensemble $A = \left\{-\frac{p-1}{2}, ..., -1, 0, 1, ..\right.$ qui forme un système de résidus modulo p. Pour tout $i \in A$, on a $i^2 = (-i)^2$. Réciproquement, si $a^2 \equiv b^2 \mod p$, alors $p \mid (a+b)(a-b)$ donc $a \equiv b \mod p$ ou $a \equiv -b \mod p$. On en déduit qu'il y a exactement $\frac{p+1}{2}$ carrés modulo p, qui sont exactement 0^2, 1^2, ..., $\left(\frac{p-1}{2}\right)^2$.

Lorsque x parcourt un système de résidus modulo p, x^2 prend donc exactement $\frac{p+1}{2}$ valeurs modulo p, et il en est de même pour $-2-y^2$. Deux ensembles de cardinal $\frac{p+1}{2}$ contenus dans un même ensemble de cardinal p ayant une intersection non vide, on peut choisir x et y de telle sorte que $x^2 \equiv -2-y^2 \mod p$. x^2+y^2+2 est alors divisible par p.

Solution de l'exercice 12 Posons $N = 2011^{2012}$. Lorsque n parcourt $\mathbb{N}$, le couple (u_n, u_{n+1}) ne peut prendre qu'un nombre fini de valeurs modulo N. Il existe donc deux entiers naturels distincts s et t (avec par exemple $s < t$) tels que $u_s \equiv u_t \mod N$ et $u_{s+1} \equiv u_{t+1} \mod N$. La définition de la suite montre que dès que $s \geqslant 1$, cela implique que $u_{s-1} \equiv u_{t-1} \mod N$. Par réccurence, on peut donc montrer que pour tout i tel que $0 \leqslant i \leqslant s$, on a $u_{s-i} \equiv u_{t-i} \mod N$. En particulier, on a $u_{t-s} \equiv u_0 \equiv 0 \mod N$ et $u_{t+1-s} \equiv u_1 \equiv 0 \mod N$, donc $n = t-s$ est solution du problème.