DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Exercices

AUTEUR : François LO JACOMO
STAGE : Grésillon 2011

Ordre modulo n, LTE : exercices

Exercice 1 Soit p un nombre premier impair. Prouver que si q est un diviseur premier de $x^{p-1} + x^{p-2} + \cdots + 1$ alors $p = q$ ou p divise $q - 1$.

Exercice 2 Soient n, k des entiers strictement positifs tels que n divise $k^n - 1$ Peut-on avoir $\text{pgcd}(n, k-1) = 1$?

Exercice 3 Soient x et y deux entiers positifs premiers entre eux. Si k est un entier impair qui divise $x^{2^n} + y^{2^n}$ avec $n \geqslant 1$, alors il existe un entier m tel que $k = 2^{n+1}m + 1$.

Exercice 4 Trouver tous les p, q premiers tels que pq divise $2^p + 2^q$.

Exercice 5 (Irlande 1996) Soient p un nombre premier et a, n des entiers strictement positifs. Prouver que si $2^p + 3^p = a^n$, alors nécessairement $n = 1$.

Exercice 6 Soit n un entier divisible par au moins deux nombres premiers impairs distincts. Montrer qu'il n'existe pas de racine primitive modulo n.

Exercice 7 Soit $n > 1$ un entier impair. Si $m \geqslant 1$ est un entier, montrer que n ne peut pas diviser $m^{n-1} + 1$.

Exercice 8 (IMO 1990/3) Trouver tous les entiers $n \geqslant 1$ tels que n^2 divise $2^n + 1$.

Exercice 9 (Bulgarie 1997) Pour un entier $n > 0$, $3^n - 2^n$ est la puissance d'un nombre premier. Montrer que n est premier.

Exercice 10 Trouver tous les nombres premiers p, q, r tels que p divise $1 + q^r$, q divise $1 + r^p$ et r divise $1 + p^q$.

- Correction -

Solution de l'exercice 1 Un tel diviseur q divise $x^p-1=(x-1)\left(x^{p-1}+x^{p-2}+...+1\right)$ donc l'ordre de x modulo q divise p premier. Si cet ordre est p, comme d'après le théorème de Fermat il divise également $q-1$, p divise $q-1$. Si l'ordre est 1, pour tout k, $x^k \equiv 1 \pmod{q}$ donc la somme des p termes : $x^{p-1}+x^{p-2}+...+1 \equiv p \pmod{q}$ est divisible par q si et seulement si q divise p, soit $q=p$.

Solution de l'exercice 2 Soit p le plus petit facteur premier de n. Modulo p, l'ordre de k divise n puisque $k^n \equiv 1 \pmod{p}$. Par ailleurs, d'après le théorème de Fermat, l'ordre de k modulo p divise $p-1$. Or p est le plus petit facteur premier de n : le seul diviseur de n strictement inférieur à p est 1. L'ordre de p, diviseur de n inférieur ou égal à $p-1$, vaut donc nécessairement 1, ce qui prouve précisément que $k \equiv 1 \pmod{p}$, donc que p divise $k-1$, de sorte que $\mathrm{PGCD}(n, k-1)$ vaut au moins p. La réponse est donc non.

Solution de l'exercice 3 k n'est pas supposé premier, mais si tous ses facteurs premiers vérifient le résultat, alors un produit de nombres congrus à $1 \pmod{2^{n+1}}$ sera lui-même $\equiv 1 \pmod{2^{n+1}}$. Il suffit donc de démontrer que tout facteur premier p de $x^{2^n}+y^{2^n}$ vérifie $p \equiv 1 \pmod{2^{n+1}}$. Par ailleurs, si p divisait x, comme par hypothèse il divise $x^{2^n}+y^{2^n}$, il diviserait également y : x et y ne seraient pas premiers entre eux. Donc x et p sont premiers entre eux et, d'après Bézout, il existe u et v tels que $xu-pv=1$, ce qui entraîne que : $xuy \equiv y \pmod{p}$. On peut noter $\left(\frac{y}{x}\right)$ la classe de $uy \pmod{p}$, telle que $x\left(\frac{y}{x}\right) \equiv y \pmod{p}$, de sorte que : $x^{2^n}+y^{2^n}=x^{2^n}\left(1+\left(\frac{y}{x}\right)^{2^n}\right) \equiv 0$ équivaut à : $\left(\frac{y}{x}\right)^{2^n} \equiv -1 \pmod{p}$. Donc cet élément $\left(\frac{y}{x}\right)$ a pour ordre 2^{n+1}, car 2^{n+1} est la première puissance de 2 vérifiant $\left(\frac{y}{x}\right)^{2^k} \equiv 1 \pmod{p}$, et 2^{n+1} n'a pas d'autre diviseur que des puissances de 2. Comme $\left(\frac{y}{x}\right)^{p-1} \equiv 1 \pmod{p}$, 2^{n+1} divise $p-1$, ce qui est précisément le résultat cherché. Un cas particulier important : pour $n=1$, tout diviseur d'une somme de deux carrés premiers entre eux est congru à 1 modulo 4.

Par ailleurs, au 17ème siècle, Fermat avait émis l'hypothèse que pour tout entier k, $2^{2^k}+1$ est premier. C'est la seule conjecture de Fermat qui s'est avérée fausse. Parmi ces "nombres de Fermat", on n'en connait que cinq qui soient premiers (pourtant, on en a étudié beaucoup) : $2^1+1=3$, $2^2+1=5$, $2^4+1=17$, $2^8+1=257$ et $2^{16}+1=65537$, et il se peut que ce soient les seuls. Pour démontrer que $2^{32}+1$ n'est pas premier, Euler savait que ses éventuels diviseurs premiers étaient nécessairement de la forme $64k+1$: il suffisait donc d'essayer $193, 257, 449, 577, 641$.... Or 641 qui peut s'écrire de deux manières : $641=\left(5\times 2^7\right)+1=5^4+2^4$. Comme $a-b$ divise a^4-b^4, 641 divise $\left(5^4\times 2^{28}\right)-$

1. Mais il divise aussi : $\left(5^4+2^4\right)\times 2^{28} = \left(5^4\times 2^{28}\right)+2^{32}$. Donc il divise la différence de ces deux nombres, à savoir précisément : $2^{32}+1$.

Solution de l'exercice 4 Remarquons tout d'abord que si $p=2$, $2q$ divise $4+2^q$ si et seulement si soit $q=2$, soit $2q$ divise 6, puisque pour tout q impair q divise $2^{q-1}-1$, donc $2q$ divise 2^q-2. D'où les solutions : $(p,q)=(2,2),(2,3)$ ou $(3,2)$. On supposera désormais p et q impairs. Appelons ω_p et ω_q les ordres de 2 modulo p et q respectivement. Si p divise 2^p+2^q, donc $2^{p-1}+2^{q-1}$, comme p divise $2^{p-1}-1$, p divise $2^{q-1}+1$, donc $2^{2(q-1)}-1$. Dès lors, ω_p divise $p-1$ et $2(q-1)$ mais ne divise pas $q-1$. Si la plus grande puissance de 2 divisant ω_p (resp ω_q) est 2^{ν_p} (resp 2^{ν_q}), le fait que ω_p divise $2(q-1)$ et pas $q-1$ entraine que $\nu_p > \nu_q$, car $q-1$ est divisible par ω_q donc par 2^{ν_q} et pas par 2^{ν_p}. Le même raisonnement, en échangeant p et q, aboutit à $\nu_q > \nu_p$, ce qui est manifestement incompatible. Il n'existe donc pas de couples de nombres premiers impairs vérifiant cette condition.

Solution de l'exercice 5 Si $p=2$, $2^2+3^2=13$ vérifie bien la relation demandée : ce n'est pas une puissance $\geqslant 2$ d'un entier. Si maintenant p est impair, 2^p+3^p est divisible par $2+3=5$, et n'est divisible par 25 que si p est divisible par 5 donc, puisque par hypothèse p est premier, si $p=5$. En effet, $3^p=(5-2)^p\equiv(-2)^p+p.5(-2)^{p-1} \pmod{25}$. C'est aussi une conséquence du théorème LTE qui se démontre pareillement. On en déduit que, hormis éventuellement pour $p=5$, le facteur 5 apparait avec l'exposant 1, ce qui suffit à démontrer le résultat cherché. Pour $p=5$, il apparait bien avec l'exposant 2, mais $3^5+2^5=275$ n'est pas une puissance $\geqslant 2$ d'un entier, ce qui achève la démonstration.

Solution de l'exercice 6 Posons $n=p^iq^jm$, p et q étant les deux nombres premiers impairs distincts et m n'étant divisible ni par p ni par q. L'anneau $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(n)=\varphi\left(p^i\right)\times\varphi\left(q^j\right)\times\varphi(m)$ éléments, et pour qu'ils soient tous atteints comme puissances d'un élément a, il faut que l'ordre de a soit $\varphi(n)$. Or $a^{\varphi\left(p^i\right)}\equiv 1 \pmod{p^i}$, $a^{\varphi\left(q^j\right)}\equiv 1 \pmod{q^j}$, $a^{\varphi(m)}\equiv 1 \pmod{m}$, donc $a^\omega\equiv 1 \pmod{n}$ avec $\omega=\mathrm{PPCM}\left(\varphi\left(p^i\right),\varphi\left(q^j\right),\varphi(m)\right)$. Comme p et q sont impairs, $\varphi\left(p^i\right)$ et $\varphi\left(q^j\right)$ sont tous deux pairs : leur PPCM ne peut pas être égal à leur produit. En définitive, l'ordre de a divise le PPCM des indicateurs d'Euler, soit au plus la moitié du nombre d'éléments inversibles qui, lui, est égal au produit de ces mêmes indicateurs d'Euler.

Solution de l'exercice 7 C'est une conséquence presque immédiate de l'exercice 3. Soit 2^k la plus grande puissance de 2 divisant $n-1$: posons $n-1=2^kq$. $s=m^{n-1}+1=x^{2^k}+y^{2^k}$ avec $x=m^q$ et $y=1$. D'après l'exercice 3, tout

diviseur de s est donc congru à 1 modulo 2^{k+1}. Or par définition de 2^k, n n'est pas congru à 1 modulo 2^{k+1}. Donc n ne divise pas s.

Solution de l'exercice 8 Montrons que si n divise $2^n + 1$, alors n est une puissance de 3. En considérant p le plus petit facteur premier de n, des considérations sur l'ordre de 2 modulo p donnent $p = 3$ comme dans les exercices du cours. Écrivons alors $n = 3^k u$ avec u non divisible par 3. Le même raisonnement montre que si $u > 1$ alors le plus petit facteur premier de u est 3. On en déduit que n est une puissance de 3.

On applique LTE (n est impair) :

$$v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = k + 1.$$

Or $v_3(n^2) = 2k$ et n^2 divise 2^n+1. On en déduit que $2k \leqslant k+1$, ce qui donne $k = 0$ ou $k = 1$. Notons que ce dernier résultat peut aussi se démontrer de manière immédiate en regardant les puissances de2 modulo 9. Réciproquement, $n = 1$ et $n = 3$ sont bien solution.

Solution de l'exercice 9 On suppose $n > 2$ et que $3^n - 2^n = p^k$ pour $k \geqslant 1$. Montrons d'abord que n est impair. Si $n = 2n'$, alors $3^n - 2^n = (3^{n'} - 2^{n'})(3^{n'} + 2^{n'})$. Il existe donc $\alpha > \beta \geqslant 0$ tels que :

$$3^{n'} + 2^{n'} = p^\alpha, \qquad 3^{n'} - 2^{n'} = p^\beta.$$

Alors $2^{n'+1} = p^\beta(p^{\alpha-\beta} - 1)$. Donc $p = 2$, ce qui est absurde. Ainsi n est impair.

Raisonnons par l'absurde et considérons q est un nombre premier divisant n avec $q < n$. Écrivons $n = qr$. Un raisonnement direct montre que $3^q - 2^q$ est une puissance de p, disons $3^q - 2^q = p^{k'}$ avec $k' < k$. En appliquant LTE, on voit que $v_p(r) = k - k'$. Écrivons donc $r = p^{k-k'}u$ avec p ne divisant pas u. Alors :

$$\begin{aligned} p^k &= 3^n - 2^n = 3^{qp^{k-k'}u} - 2^{qp^{k-k'}u} = (3^q)^{p^{k-k'}u} - (2^q)^{p^{k-k'}u} \\ &= (p^{k'} + 2^q)^{p^{k-k'}u} - (2^q)^{p^{k-k'}u} \geqslant p^{k-k'}u \cdot p^{k'} \cdot 2^{q(p^{k-k'}u-1)} = p^k u \cdot 2^{q(p^{k-k'}u-1)} > p^k, \end{aligned}$$

ce qui est absurde. n est donc forcément premier.

Solution de l'exercice 10 On commence par examiner la condition « p divise $1 + q^r$ ». Elle se réecrit $q^r \equiv -1 \bmod p$ et implique donc, en particulier, $q^{2r} \equiv 1 \bmod p$. Ainsi l'ordre de q modulo p est un diviseur de $2r$. Comme r est supposé premier, c'est donc un élément de l'ensemble $\{1, 2, r, 2r\}$. Si on suppose en outre que $p \neq 2$, on a $q^r \neq 1 \bmod p$, et donc l'ordre de q modulo p est nécessairement

2 ou r. Dans le premier cas, en utilisant que p est premier, on obtient $q \equiv -1 \bmod p$, alors que dans le deuxième cas, on en déduit que $2r$ divise $p-1$. En permutant les nombres p, q et r, on obtient bien sûr des conséquences analogues des deux autres conditions « q divise $1+r^p$ » et « r divise $1+p^q$ ».

On suppose maintenant que p, q et r sont tous les trois impairs, et pour commencer que l'on est dans le cas où $q \equiv -1 \bmod p$. Le nombre premier p ne peut donc pas diviser $q-1$ (puisqu'il divise déjà $q+1$ et qu'il ne vaut pas 2). D'après les résultats du premier alinéa, la condition « q divise $1+r^p$ » implique donc que $r \equiv -1 \bmod q$. En appliquant à nouveau le même argument, on trouve que $p \equiv -1 \bmod r$. Or les trois congruences précédentes ne sont pas compatibles. En effet, par exemple, elles impliquent $q \geqslant p-1$, $r \geqslant q-1$ et $p \geqslant r-1$, ce qui ne peut se produire, étant donné que p, q et r sont des nombres premiers impairs, que si $p = q = r$; on a alors manifestement $q \not\equiv -1 \bmod p$. On en déduit que, toujours dans le cas où p, q et r sont supposés impairs, $2r$ divise $p-1$. En permutant circulairement les variables, on démontre de même que $2p$ divise $q-1$ et $2q$ divise $r-1$. Ainsi $8pqr$ divise $(p-1)(q-1)(r-1)$, ce qui n'est clairement pas possible étant donné que $8pqr > (p-1)(q-1)(r-1)$. Finalement, il n'y a pas de solution lorsque p, q et r sont tous les trois impairs.

On en vient à présent au cas où l'un de ces trois nombres est égal à 2. Quitte à permuter circulairement à nouveau p, q et r, on peut supposer que c'est p. Les conditions de l'énoncé disent alors que q est impair, que $r^2 \equiv -1 \bmod q$ et que $2^q \equiv -1 \bmod r$. Par ce qui a été fait dans le premier alinéa, cette dernière congruence entraîne que $r = 3$ ou que $2q$ divise $r-1$. Le premier cas conduit à $9 \equiv -1 \bmod q$, ce qui ne se produit que si $q = 5$ puisque l'on a déjà écarté le cas $q = 2$. On vérifie par ailleurs que le triplet $(2, 5, 3)$ est bien solution. Dans le second cas, maintenant, le produit $2q$ divise $r-1$, mais aussi $2(r^2+1)$ puisqu'on sait que $r^2 \equiv -1 \bmod q$. Ainsi $2q$ divise $2(r^2+1)-2(r+1)(r-1) = 4$, ce qui ne peut arriver.

En conclusion, il y a exactement trois solutions qui sont les triplets $(2, 5, 3)$, $(5, 3, 2)$ et $(3, 2, 5)$.