DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Exercices

AUTEUR : Thomas BUDZINSKI
STAGE : Montpellier 2013

Valuations p-adiques, congruences

Vu en cours :
- Existence et unicité de la décomposition en facteurs premiers
- Valuation p-adique, lien avec la divisibilité, le PGCD, le PPCM...
- Existence d'une infinité de nombres premiers
- Congruences
- Théorème chinois

Pour plus de détails, vous pouvez consulter le poly d'arithmétique disponible à l'adresse ci-dessous :
http://www.animath.fr/spip.php?article255

Exercice 1 Calculer le nombre de diviseurs d'un entier en fonction de sa décomposition en facteurs premiers.

Solution de l'exercice 1 Soit $n = p_1^{\alpha_1}...p_k^{\alpha_k}$: choisir un diviseur de n revient à choisir des entiers naturels $\beta_1, ..., \beta_k$ avec $\beta_i \leqslant \alpha_i$ pour tout i. Il y a $\alpha_1 + 1$ choix pour β_1 etc..., donc le nombre de diviseurs de n vaut $(\alpha_1 + 1)...(\alpha_k + 1)$.

Exercice 2 Soient a et b dans $\mathbb{N}^*$ tels que $a^n | b^{n+1}$ pour tout n de $\mathbb{N}$.
Montrer que $a|b$.

Solution de l'exercice 2 On utilise les valuations p-adiques : la condition signifie que pour tous p et n, $\nu_p(a) \leqslant \left(1 + \frac{1}{n}\right) \nu_p(b)$ d'où, en passant à la limite, $\nu_p(a) \leqslant \nu_p(b)$ et ce pour tout p premier, donc $a|b$.

Exercice 3 (IMO 2009) Soient $k \geqslant 2$, n dans $\mathbb{N}^*$ et a_1, a_2, ..., a_k deux à deux distincts dans $[\![1, n]\!]$ tels que n divise $a_1(a_2 - 1)$, $a_2(a_3 - 1)$, ..., $a_{k-1}(a_k - 1)$.
Montrer que n ne divise pas $a_k(a_1 - 1)$.

Solution de l'exercice 3 On fixe n et on raisonne par récurrence sur k : pour $k =$

2, si n divise $a(b-1)$ et $b(a-1)$, alors n divise $a-b$ donc $a=b$, ce qui est impossible.
Si le résultat est vrai pour $n-1$, on sait que n ne divise pas $a_{k-1}(a_1-1)$. Il existe donc p tel que $v_p(a_{k-1})+v_p(a_1-1)<v_p(n)$. Or, on sait que $v_p(a_{k-1})+v_p(a_k-1)\geqslant v_p(n)$.
On a donc :

$$v_p(a_{k-1})+v_p(a_k-1)\geqslant v_p(n)>v_p(a_{k-1})+v_p(a_1-1)\geqslant v_p(a_{k-1})$$

donc $v_p(a_k-1)>0$ donc, comme a_k et a_k-1 sont premiers entre eux, $v_p(a_k)=0$ donc :

$$v_p(a_k)+v_p(a_1-1)=v_p(a_1-1)\leqslant v_p(a_1-1)+v_p(a_{k-1})<v_p(n)$$

donc n ne divise pas $a_k(a_1-1)$.

Exercice 4 Trouver tous les triplets d'entiers (x,y,z) tels que :

$$x^2+y^2+1=2^z$$

Solution de l'exercice 4 On regarde modulo 4 : on vérifie qu'on a $x^2\equiv 0 \pmod 4$ si x est pair et $x^2\equiv 1 \pmod 4$ si x est impair, donc x^2+y^2 est congru à 0, 1 ou 2 modulo 4, donc le membre de gauche n'est jamais divisible par 4, ce qui impose $z\leqslant 1$, donc x^2+y^2 vaut 0 ou 1.

Exercice 5 Soient $A=2012^{2012}$, B la somme des chiffres de A, C la somme des chiffres de B et D la somme des chiffres de C.
Combien vaut D ?

Solution de l'exercice 5 On a $2012\equiv 5 \pmod 9$ d'où $2012^{2012}\equiv 5^{2012} \pmod 9$. On étudie donc les puissances de 5 modulo 9 : $5^2\equiv 7$ donc $5^3\equiv -1$ et $5^6\equiv 1$. Or, on peut écrire $2012=2+6*335$, d'où :

$$2012^{2012}\equiv 5^{2012}\equiv 5^2*(5^6)^{335}\equiv 5^2\equiv 7 \pmod 9$$

donc $D\equiv C\equiv B\equiv A\equiv 7 \pmod 9$.
D'autre part, $A<(10^4)^{2012}=10^{8048}$ donc A a au plus 8048 chiffres donc $B\leqslant 9*8048=72432$, donc B a au plus 5 chiffres, donc $C\leqslant 45$, et $D\leqslant 13$. La seule possibilité est donc $D=7$.

Exercice 6 Refaire l'exercice 3 en utilisant des congruences.

Solution de l'exercice 6 L'hypothèse s'écrit $a_i a_{i+1} \equiv a_i \pmod{n}$ pour tout i donc :

$$a_1 \equiv a_1 a_2 \equiv a_1 a_2 a_3 \equiv ... \equiv a_1 ... a_k \pmod{n}$$

Or, si n divisait $a_k(a_1 - 1)$, on aurait $a_k a_1 \equiv a_k \pmod{n}$ et on pourrait écrire :

$$a_2 \equiv a_2 a_3 \equiv ... \equiv a_2 a_3 ... a_k \equiv a_2 ... a_n a_1 \pmod{n}$$

d'où $a_1 \equiv a_2 \pmod{n}$ donc $a_1 = a_2$ (car a_1 et a_2 sont dans $[\![1, n]\!]$...), ce qui est en contradiction avec l'énoncé.

Exercice 7 Un point du plan de coordonnées entières (p, q) est dit invisible si $\text{PGCD}(p, q) > 1$.
Soit $n \in \mathbb{N}$. Montrer qu'il existe un carré de côté n dans lequel tous les points à coordonnées entières sont invisibles.

Solution de l'exercice 7 On cherche a et b tels que pour tous i et j de $[\![0, n-1]\!]$, $a + i$ et $b + j$ ne soient pas premiers entre eux. Soient donc $(p_{i,j})_{i,j \in [\![0,n-1]\!]}$ n^2 nombres premiers deux à deux distincts : on veut que pour tous i et j, $a + i$ et $b + j$ soient tous deux divisibles par $p_{i,j}$, soit $a \equiv -i \pmod{p_{i,j}}$ pour tous i et j et $b \equiv -j \pmod{p_{i,j}}$. L'existence de tels a et b est garantie par le théorème chinois.

Exercice 8 Soit $n > 0$. Montrer qu'il existe n entiers consécutifs, dont aucun n'est une puissance parfaite.

Solution de l'exercice 8 On cherche à transformer le problème en problème sur les congruences : pour qu'un nombre m ne soit pas une puissance parfaite, il suffit qu'il existe p premier tel que $\nu_p(m) = 1$, ce qui est par exemple le cas si $m \equiv p \pmod{p^2}$. Soient donc p_1, p_2, ..., p_n n nombres premiers distincts (car il y a n conditions à vérifier). D'après le théorème chinois, il existe m tel que :

$$\begin{cases} m \equiv p_1 \pmod{p_1^2} \\ m \equiv p_2 - 1 \pmod{p_2^2} \\ \quad ... \\ m \equiv p_n - (n-1) \pmod{p_n^2} \end{cases}$$

On a alors, pour tout i de $[\![0, n-1]\!]$, $m + i \equiv p_i \pmod{p_i^2}$ donc $m + i$ n'est pas une puissance parfaite.