DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Exercices

AUTEUR : Bodo LASS
STAGE : Grésillon 2011

Invariants, Principe des tiroirs

Exercice 1 Trouvez le PGCD de tous les nombres de la forme $n^{13} - n$.

Exercice 2 Trouvez tous les entiers x, y, z tels que

$$3x^2 + 7y^2 = z^4$$

Exercice 3 Montrez que la fraction $\frac{39n+4}{26n+3}$ est toujours irréductible.

Exercice 4 (théorème de Wilson) Soit p un premier.

1. Montrez que dans $\mathbb{Z}/p\mathbb{Z}$ tous les éléments non nuls ont un inverse, c-à-d pour tout entier k non divisible par p, il existe un entier l tel que

$$k \cdot l \equiv 1[p].$$

2. Montrez que

$$n \text{ premier } \Leftrightarrow (n-1)! \equiv -1[n]$$

Exercice 5 On note $[x]$ la partie entière de x, et on choisit n un entier, montrez que

$$\left[\sqrt{n} + \sqrt{n+1}\right] = \left[\sqrt{4n+2}\right]$$

Exercice 6 Montrez que pour tout premier p et tout entier $0 < k < p$, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ est divisible par p.

Exercice 7 Calculez la somme infinie suivante :

$$\left[\frac{x+1}{2}\right] + \left[\frac{x+2}{4}\right] + \left[\frac{x+4}{8}\right] + \left[\frac{x+8}{16}\right] + \dots$$

Question intermédiaire : montrez que $[2x] = [x] + [x + 1/2]$.

Exercice 8 Montrez que pour tout entier n,

$$n! \text{ divise } \prod_{k=0}^{n-1}(2^n - 2^k)$$

- Correction -

Solution de l'exercice 1 Nous allons chercher tous les premiers qui divisent $n^{13} - n$ pour tout n, c-à-d $p|(n^{12} - 1)$ pour tout n premier avec p. Le petit théorème de Fermat dit que $p|(n^{p-1} - 1)$, donc si $(p - 1)|12$, alors $p|(n^{12} - 1)$ pour tout n premier avec p. On a au moins $p = 2, 3, 5, 7$ et 13. Maintenant montrons que p^2 ne divise pas $n^{13} - n$ pour tout n avec un cas particulier : p^2 divise p^{13} mais pas p donc p^2 ne divise pas $p^{13} - p$. La dernière étpe est de montrer qu'il n'y a pas d'autre facteur premier. La solution idéale serait de montrer la réciproque du théorème de Fermat, mais ici il suffit d'observer que $2^{13} - 2 = 8190 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. Le plus grand diviseur commun est donc $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730$.

Solution de l'exercice 2 Nous allons nous intéresser à une équation un peu plus générale :

$$3x^2 + 7y^2 = n^2$$

Si (x, y, z) est une solution de la premère équation alors $(x, y, n = z^2)$ est solution de la seconde. Rappelons-nous que le carré d'un entier est congru à 0 ou 1 modulo 4. En essayant les 8 cas possibles, on aboutit à la conclusion que x, y et n sont tous les trois pairs.

À présent nous allons utiliser la méthode de la descente infinie : supposons qu'il existe des solutions non nulles. Alors on peut choisir une solution (x, y, n) où n est minimal (et strictement positif). D'après le paragraphe précédent, x, y et n sont tous pairs. De plus, le triplet $(x', y', n') = (\frac{x}{2}, \frac{y}{2}, \frac{n}{2})$ est également solution de l'équation, ce qui contredit la minimalité de (x, y, n). Il n'y a donc pas de solutions non nulles à cette équation.

Solution de l'exercice 3 Si un entier k divise $39n + 4$ et $26n + 3$, alors il divise aussi $3(26n + 3) - 2(39n + 4) = 1$, donc $k = 1$.

Solution de l'exercice 4 Soit p un premier.

1. Soit $1 \leqslant k \leqslant p-1$, la famille $\{0, k, 2k, \ldots, (p-1)k\}$ est une famille complète de résidus modulo p, donc il existe un (unique) entier $1 \leqslant l \leqslant p-1$ tel que $kl \equiv 1 \bmod p$.
2. Tout d'abord, si p n'est pas premier alors il a un diviseur $d \in \{2, \ldots, p-1\}$, donc d divise $(p-1)!$. Cette factorielle ne peut donc pas être congrue à $(-1) \bmod p$.

   À présent prenons p premier. On va ranger les $p-1$ entiers en couples (k, l) tels que $kl \equiv 1[p]$. Il fau vérifier que l'on a pas des couples (k, k) : si $k^2 \equiv 1[p]$ cela signifie que $p|k^2 - 1 = (k+1)(k-1)$ donc soit $p|k-1$, soit $p|k+1$, les seuls entiers problématiques sont donc 1 et $p-1$, tous les autres peuvent se placer en couples, on en conclut que $2 \cdot 3 \ldots (p-2) \equiv 1[p]$. Et on a bien $(p-1)! \equiv -1[p]$.

Solution de l'exercice 5 Raisonnons par l'absurde, supposons qu'il existe un entier k tel que

$$\sqrt{n} + \sqrt{n+1} < k \leqslant \sqrt{4n+2}.$$

En mettant ces inégalités au carré, on obtient

$$2n + 1 + 2\sqrt{n(n+1)} < k^2 \leqslant 4n + 2$$

Ensuite on utilise $n = \sqrt{n^2} \leqslant \sqrt{n(n+1)}$

$$2n + 1 + 2n < k^2 \leqslant 4n + 2$$

Comme k^2 est un entier, la seule solution est que $k^2 = 4n + 2$. Mais il n'existe pas de carré congru à 2 mod 4, contradiction !

Solution de l'exercice 6

$$p! = \binom{p}{k} \cdot k! \cdot (p-k)!$$

L'entier premier p divise $p!$, mais ni $k!$ ni $(p-k)!$ puisque $1 \leqslant k \leqslant p-1$. Donc p divise $\binom{p}{k}$

Solution de l'exercice 7 Commençons l'observation que cette somme est finie. En effet, si $2^k > x$ alors $x + 2^k < 2^{k+1}$ et finalement $\left[\frac{x+2^k}{2^{k+1}}\right] = 0$. Passons maintenant à la question intermédiaire. On fait simplement une disjonction de cas : si $n \leqslant x < n + 1/2$ alors $[2x] = 2n$ et $[x] + [x + 1/2] = n + n$, et si $n + 1/2 \leqslant x < n + 1$ alors $[2x] = 2n + 1$ et $[x] + [x + 1] = n + (n + 1)$. Sur le terme de la suite, ca permet d'avoir

$$\left[\frac{x + 2^k}{2^{k+1}}\right] = \left[\frac{x}{2^{k+1}} + \frac{1}{2}\right] = \left[2\frac{x}{2^{k+1}}\right] - \left[\frac{x}{2^{k+1}}\right]$$

$$\left[\frac{x+1}{2}\right] + \left[\frac{x+2}{4}\right] + \cdots = \left([x] - \left[\frac{x}{2}\right]\right) + \left(\left[\frac{x}{2}\right] - \left[\frac{x}{4}\right]\right) + \dots$$

et les termes son téléscopiques, à la fin il ne reste que $[x]$.

Solution de l'exercice 8 Pour gagner de la place on note

$$A_n = \prod_{k=0}^{n-1} (2^n - 2^k)$$

Pour tout premier p on note $\nu_p(A_n)$ la valuation p-adique de A_n (c-à-d l'exposant de p dans sa décomposition en facteurs premiers). On veut montrer qu'elle est supérieure à celle de $n!$. Utilisons la formule de Legendre :

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \left[\frac{n}{p^4}\right] + \dots$$

On remarque d'abord que $\left[\frac{n}{p^k}\right] \leqslant \frac{n}{p^k}$, donc

$$\nu_p(n!) \leqslant \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} \cdots = \frac{n}{p-1}$$

Comparons avec $\nu_p(A_n)$. Débarassons nous du cas $p = 2$

$$A_n = \prod_{k=0}^{n-1} (2^n - 2^k) = \prod_{k=0}^{n-1} 2^k (2^{n-k} - 1)$$

donc $\nu_2(A_n) = \frac{n(n-1)}{2}$. Maintenant, pour p impair : $(2^{n-k} - 1)$ est un multiple de p à chaque fois que $(n-k)$ est un multiple de p, ce qui arrive $\left[\frac{n}{p-1}\right]$ fois. On a donc

$$\nu_p(n!) \leqslant \frac{n}{p-1} \text{ et } \left[\frac{n}{p-1}\right] \leqslant \nu_p(A_n)$$

On a presque l'inégalité souhaitée, à une partie entière près, mais comme les valuations sont des entiers, on est bons !