DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Exercices

AUTEUR : Matthieu LEQUESNE
STAGE : Montpellier 2014

Exercices d'arithmétiques

Durant ce TD d'arithmétique, nous avons fini de corriger les exercices de dimanche. Les exercices suivants ont également été traités :

Exercice 1 Calculer le nombre de 0 à la fin de 2014 !

Exercice 2 Montrer que la somme de cinq carrés d'entiers consécutifs n'est jamais un carré parfait.

Exercice 3 Montrer qu'il existe une infinité d'entiers $a \geqslant 0$ tels que $n^4 + a$ n'est premier pour aucun n.

Exercice 4 On note $P(n)$ le produit des diviseurs de n et $d(n)$ le nombre de diviseurs de n. Montrer que $P(n) = n^{d(n)/2}$.

Exercice 5 Soit $n = \prod p_i^{\alpha_i}$. Montrer que le nombre de diviseurs de n est $\prod(\alpha_i + 1)$.

Exercice 6 Soit $a \geqslant 1$ et $b \geqslant 2$ tels que $a^b - 1$ est premier. Montrer que $a = 2$ et b est premier.

Exercice 7 Quels sont les deux derniers chiffres de $7^{9^{9}}$?

Exercice 8 Donner une condition nécessaire et suffisante sur p et q pour que $x \in \mathbb{Q}$ si et seulement si $x^p \in \mathbb{Q}$ et $x^q \in \mathbb{Q}$.

Exercice 9 Soit $a \geqslant 2$, $m \geqslant n \geqslant 1$.

a) Montrer que PGCD$(a^m - 1, a^n - 1)$ = PGCD$(a^{m-n} - 1, a^n - 1)$.
b) Montrer que PGCD$(a^{m-1}, a^n - 1)$ = $a^{\text{PGCD}(m,n)} - 1$.
c) Montrer que $a^m - 1 \mid a^n - 1 \Leftrightarrow m \mid n$.

Exercice 10 Montrer que $\prod_{k=0}^{n-1}(2^n - 2^k)$ est divisible par $n!$.

Exercice 11 (Théorème de Wilson) Soit p un entier > 1. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.

Solution de l'exercice 1 Comme $10 = 2 \times 5$ cela revient à calculer $\min(\nu_2(2014!), \nu_5(2014$
Or il y a plus de facteurs 2 que de facteurs 5. Donc on calcule $\nu_5(2014!)$ à l'aire de la formule de Legendre :

$$\nu_5(2014!) = \sum_{k=1}^{+\infty} \lfloor \frac{2014}{5^k} \rfloor = 501$$

Solution de l'exercice 2 Sachant qu'un carré est congru à 0 ou 1 modulo 4, la somme de cinq carrés d'entiers consécutifs est congrue à 2 ou 3 modulo 4.

Solution de l'exercice 3 On prend $a = 4b^4$ donc $n^4 + a = (n^2 + 2b^2 + 2nb)(n^2 + 2b^2 - 2nb)$.

Solution de l'exercice 4 $P(n)^2 = \prod_{d|n} d \times \prod_{d|n} \frac{n}{d} = \prod_{d|n} n = n^{d(n)}$.

Solution de l'exercice 5 Les diviseurs de n sont les nombres de la forme $\prod p_i^{\beta_i}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$. Il y en a donc $\prod(\alpha_i + 1)$.

Solution de l'exercice 6 $a^b - 1$ est divisible par $a - 1$ donc nécessairement $a = 2$. De plus si $b = cd$, $2^b - 1$ est divisible par $2^c - 1$ donc $c = 1$ ou $c = b$. Donc b est premier.

Solution de l'exercice 7 On regarde les restes des puissances de 7 modulo 100. C'est un cycle de longueur 4. Or $9 \equiv 1 \pmod{4}$ donc les deux derniers chiffres sont 07.

Solution de l'exercice 8 Si $\mathrm{PGCD}(p, q) = d > 1$, $\sqrt[d]{2}$ est un contre-exemple. Si $\mathrm{PGCD}(p, q) = 1$, il existe u et v tels que $pu + qv = 1$ d'après le théorème de Bézout. Donc $x = (x^p)^u + (x^q)^v$ est rationnel.

Solution de l'exercice 9

a) $\mathrm{PGCD}(a^m - 1, a^n - 1) = \mathrm{PGCD}(a^n(a^{m-n} - 1), a^n - 1) = \mathrm{PGCD}(a^{m-n} - 1, a^n - 1)$ car a^n et $a^n - 1$ sont premiers entre eux..

b) On applique l'algorithme des soustractions.

c) $a^m - 1 \mid a^n - 1 \Leftrightarrow \mathrm{PGCD}(a^m - 1, a^n - 1) = a^m - 1 \Leftrightarrow \mathrm{PGCD}(m, n) = m \Leftrightarrow m \mid n$.

Solution de l'exercice 10 $\prod_{k=0}^{n-1}(2^n - 2^k) = 2^{\frac{n(n-1)}{2}} \prod_{k=0}^{n-1}(2^k - 1)$. Or $\nu_2(n!) < n < \frac{n(n-1)}{2}$.

De plus, si $p \geqslant 3$, alors $v_p(2^k - 1) \geqslant a$ dès que k est un multiple de $\varphi(p^a) = (p-1)p^{a-1}$ (où φ est l'indicatrice d'Euler) : il y a au moins $\lfloor \frac{n}{(p-1)p^{a-1}} \rfloor$ tels entiers k. De manière analogue à la formule de Legendre, on sait donc que $v_p(\prod_{k=0}^{n-1}(2^k - 1)) \geqslant \lfloor \frac{n}{p-1} \rfloor + \lfloor \frac{n}{p(p-1)} \rfloor + \ldots$ Or, $v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots$ (c'est la formule de Legendre), donc $v_p(n!) \leqslant v_p(\prod_{k=0}^{n-1}(2^k - 1))$. Cela montre bien que $n!$ divise $\prod_{k=0}^{n-1}(2^n - 2^k)$.

Solution de l'exercice 11 Pour tout $n \in [\![1, p-1]\!]$, il existe $n^{-1} \in [\![1, p-1]\!]$ tel que $n \times n^{-1} \equiv 1[p]$. De plus, $n = n^{-1}$ si et seulement si $n^2 - 1 \equiv 0$, ce qui équivaut à $n = 1$ ou $n = p - 1$.

Ainsi, calculer $(p-1)!$ modulo p revient :

- si $n \neq n^{-1}$, à grouper chaque entier n avec son inverse n^{-1} pour les multiplier, ce qui produit uniquement des facteurs 1 modulo p,
- sinon, c'est que $n = 1$ ou $n = p - 1$, ce qui rajoute un facteur 1 et un facteur -1 modulo p.

Donc : $(p-1)! \equiv 1 \times 1 \times \ldots \times 1 \times 1 \times (-1) \equiv -1[p]$.