DOMAINE : Arithmétique
NIVEAU : Intermédiaire
CONTENU : Cours et exercices

AUTEUR : Thomas BUDZINSKI
STAGE : Montpellier 2014

Ordre modulo n

1 Résumé du cours

Définition 1. Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ premiers entre eux. L'*ordre de* a *modulo* n est le plus petit entier $d > 0$ tel que $a^d \equiv 1 \pmod{n}$.

Proposition 2. L'ordre est bien défini, i.e il existe bien d tel que $a^d \equiv 1 \pmod{n}$. De plus, soit $k \in \mathbb{N}$: alors $a^k \equiv 1 \pmod{n}$ si et seulement si k divise n.

Remarque 3. ATTENTION ! ! ! Si $a^k \equiv 1 \pmod{n}$, cela ne veut pas forcément dire que k est l'ordre de a modulo n. La seule chose qu'on peut conclure est que l'ordre de a est un diviseur de k.

Théorème 4. (Petit théorème de Fermat) Soient p premier et a non divisible par p. Alors $a^{p-1} \equiv 1 \pmod{p}$. Autrement dit, l'ordre de a modulo p est un diviseur de $p-1$.

Définition 5. Soit $n \geqslant 2$. On note φ de n le nombre d'entiers entre 0 et n qui sont premiers avec n. φ est appelée *fonction indicatrice d'Euler*.

Proposition 6. Si $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ avec les p_i premiers, alors :

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}...(p_k - 1)p_k^{\alpha_k - 1} = \Big(1 - \frac{1}{p_1}\Big)...\Big(1 - \frac{1}{p_k}\Big)n$$

Théorème 7. (Théorème d'Euler) Soient n et a premier avec n. Alors $a^{\varphi(n)} \equiv 1 \pmod{n}$. Autrement dit, l'ordre de a est un diviseur de $\varphi(n)$.

2 Exercices :

Exercice 1 (Théorème de Wilson) Soit p un nombre premier. Montrer que :

$$(p-1)! \equiv -1 \pmod{p}$$

Solution de l'exercice 1 En faisant le produit, on peut regrouper chaque élément de $(\mathbb{Z}/p\mathbb{Z})^*$ avec son inverse. Le produit vaut alors 1. Il ne reste alors que les termes qui sont leur propre inverse, c'est-à-dire tels que $x^2 = 1$, c'est-à-dire 1 et -1 (si $p = 2$ ce n'est pas tout à fait vrai car $1 = -1$ mais alors le résultat est trivial). Le produit modulo p vaut donc $1 \times 1 \times (-1) = -1$

Exercice 2 Soit $n \in \mathbb{N}^*$ premier avec 10. Montrer qu'il existe un multiple de n qui ne s'écrit qu'avec des 1.

Solution de l'exercice 2 Le nombre qui s'écrit avec k chiffres 1 est $11...1 = \frac{99...9}{9} = \frac{10^k-1}{9}$. On cherche donc k tel que $n|\frac{10^k-1}{9}$, i.e $9n|10^k - 1$. D'après ce qu'on a vu en cours, il suffit de choisir pour k l'ordre de 10 modulo $9n$. Il existe bien car 10 est premier avec 9 et n, donc avec $9n$.

Exercice 3 Soit $n \in \mathbb{N}^*$ impair. Montrer que $n|2^{n!} - 1$.

Solution de l'exercice 3 On sait que l'ordre de 2 modulo n existe car n est impair, et divise $\varphi(n)$. Comme $\varphi(n) \leqslant n$, $\varphi(n)|n!$ donc $2^{n!} \equiv 1 \pmod{n}$.

Exercice 4 Soient p un nombre premier et q un diviseur premier de $p^{p-1} + ... + p + 1$. Montrer que $q \equiv 1 \pmod{p}$.

Solution de l'exercice 4 Soit d l'ordre de p modulo q : on a $q|p^p - 1$ donc $d|p$, donc d vaut 1 ou p. Si $d = p$, alors $d|q - 1$ d'après le petit théorème de Fermat donc $q \equiv 1 \pmod{p}$ et on a gagné.

Si $d = 1$, alors $q|p - 1$. Cependant, $p^{p-1} + ... + p + 1 \equiv 1 + ... + 1 + 1 \equiv p \equiv 1 \pmod{p - 1}$, donc $p - 1$ et $p^{p-1} + ... + p + 1$ sont premiers entre eux, d'où la contradiction car q divise les deux, donc forcément on est dans le premier cas et $q \equiv p \pmod{1}$.

Exercice 5 Trouver tous les $n \in \mathbb{N}^*$ tels que n divise $2^n - 1$.

Solution de l'exercice 5 Soient $n > 1$ tel que n divise $2^n - 1$, et p le plus petit diviseur premier de n. On note d l'ordre de 2 modulo p : on sait que d divise $p - 1$, et d'autre part d'après l'énoncé $p|2^n - 1$ donc d divise n, donc d divise $\mathrm{PGCD}(n, p - 1)$.

Or, comme p est minimal, $p-1$ est plus petit que tous les diviseurs premiers de n, donc n et $p - 1$ n'ont aucun diviseur premier commun, donc leur PGCD vaut 1, donc $d = 1$. Autrement dit, $2 \equiv 1 \pmod{p}$ donc $p = 1$, ce qui est absurde, donc seul $n = 1$ est solution.

Exercice 6 Trouver tous les $n \in \mathbb{N}^*$ impairs tels que n divise $3^n + 1$.

Solution de l'exercice 6 Tout d'abord, $n = 1$ est solution.

De plus, soit q le plus petit diviseur premier de n et d l'ordre de 3 modulo q : n est impair donc $q > 2$. D'une part $d|q-1$ et d'autre part $3^n \equiv -1 \pmod{q}$ donc $3^{2n} \equiv 1 \pmod{n}$ donc $d|2n$ donc d divise le PGCD de $2n$ et $q-1$, qui vaut 2 pour les mêmes raisons que dans l'exercice précédent, donc d vaut 1 ou 2, donc $q|3^2 - 1 = 8$ donc $q = 2$, ce qui est absurde car n est impair.

$n = 1$ est donc la seule solution.

Exercice 7 Trouver tous les couples d'entiers (a, n) tels que n divise $(a+1)^n - a^n$.

Solution de l'exercice 7 Si $n = 1$, tout a convient.

Sinon, soit q le plus petit diviseur premier de a. q divise $(a+1)^n - a^n$, donc dans $\mathbb{Z}/q\mathbb{Z}$, $(a+1)^n = a^n$. Or, si $q|a$ alors $q|a^n$ donc $q|(a+1)^n$ donc $q|a+1$ et $q|1$, ce qui est absurde. a est donc inversible, et on peut écrire $\left(1 + \frac{1}{a}\right)^n = 1$. Soit donc d l'ordre de $1+\frac{1}{a}$ modulo q : d divise n et $q-1$ donc $d = 1$ et $1+\frac{1}{a} = 1$ soit $\frac{1}{a} = 0$, ce qui est absurde.

Les seules solutions sont donc $(1, a)$.

Exercice 8 Trouver tous les couples d'entiers (n, p) avec p premier, $0 < n \leqslant 2p$ et :

$$n^{p-1}|(p-1)^n + 1$$

Solution de l'exercice 8 Si $n = 1$, il faut $1|p$ ce qui est vrai pour tout p premier, donc $(1, p)$ est solution pour tout p premier.

Sinon, soit q le plus petit diviseur premier de n. Si $q = 2$, alors n est pair donc $(p-1)^n + 1$ aussi, donc $p - 1$ est impair et $p = 2$, donc $n|2$ et on a la solution $(2, 2)$.

Sinon, $q \geqslant 3$ et on note d l'ordre de $p - 1$ modulo q. D'une part, d divise $q-1$, donc est premier avec n par minimalité de q. D'autre part, $(p-1)^n \equiv -1 \pmod{q}$ donc $(p-1)^2 n \equiv 1 \pmod{q}$, donc d divise $2n$ mais pas n, donc $d = 2$. Autrement dit, q ne divise pas $(p-1) - 1 = p - 2$, mais q divise $(p-1)^2 - 1 = p(p-2)$, donc $q|p$ et $q = p$, i.e $p|n$.

Comme $n \leqslant 2p$, on a $n = p$ ou $n = 2p$, mais si $n = 2p$ alors $q = 2$ et on a supposé le contraire, donc $n = p$ et $p^{p-1}|(p-1)^p + 1$. En développant avec le binôme de Newton, on obtient :

$$p^p - \binom{p}{1} + ... + \binom{p}{p-3}p^3 - \binom{p}{p-2}p^2 + \binom{p}{p-1}p - 1 + 1$$

Tous les termes sont divisibles par p^3 sauf éventuellement les trois derniers. L'antépénultième vaut $\frac{p(p-1)}{2}p^2$ donc est divisible par p^3, donc $(p-1)^p+1 \equiv p^2 \pmod{p^3}$, donc n'est pas divisible par p^3. Il faut donc que $p-1<3$, donc $p=2$ ou $p=3$.

Les solutions sont donc finalement $(1,p)$ pour tout p premier, $(2,2)$ et $(3,3)$.

Exercice 9 Soit p un nombre premier. Montrer qu'il existe n tel que p divise :

$$2^n+3^n+6^n-1$$

Solution de l'exercice 9 On peut prendre $n=1$ pour $p=2$ et $n=2$ pour $p=3$.

Pour $p>3$, on prend $n=p-2$. Alors 2, 3 et 6 sont premiers avec p et :

$$2^{p-2}+3^{p-2}+6^{p-2}-1 \equiv \frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1 \equiv \frac{3+2+1-6}{6} \equiv 0 \pmod{p}$$