DOMAINE : Arithmétique
NIVEAU : Intermédiaire
CONTENU : Cours et exercices

AUTEUR : Samuel BACH
STAGE : Montpellier 2013

Congruences

- Calculs de PGCD -

On note (a, b) le PGCD des entiers a et b. On rappelle que $(a, b) = (a, b + ca)$ avec a, b, c des entiers. Ceci est à la base de l'algorithme d'Euclide pour calculer le pgcd de deux entiers : si $a = bq + r$, $0 \leqslant r < a$ est la division euclidienne de a par b, $(a, b) = (r, b) = (b, r)$, et en calculant ainsi la suite des restes de la division euclidienne du premier argument par le second, on obtient une suite de restes positifs strictement décroissante, qui aboutit donc à 0. La dernière étape de calcul donne ainsi un entier naturel d tel que $(a, b) = (d, 0) = d$, et on a ainsi calculé le pgcd de a et b.

Exercice 1 Soit a, b deux entiers premiers entre eux, alors $(\frac{a^n - b^n}{a-b}, a - b) = (a - b, n)$.

Solution de l'exercice 1 $(\frac{a^n - b^n}{a-b}, a - b) = (a - b, \sum_{k=0}^{n-1}(a^k b^{n-k} - b^n) + nb^n) = (a-b, \sum_{k=0}^{n-1} b^{n-k}(a^k - b^k) + nb^n) = (a-b, nb^n)$ car $a-b \mid a^k - b^k$. Comme a et b sont premiers entre eux, $a-b$ et b sont premiers entre eux, donc $(a-b, nb^n) = (a - b, n)$, ce qui conclut.

Exercice 2 Calculer le pgcd de $a^n - 1$ et $a^m - 1$.

Solution de l'exercice 2 Soit $n = mq + r$, $0 \leqslant r < m$ la division euclidienne de n par m. On a alors $a^n - 1 = a^r(a^{mq} - 1) + a^r - 1$ donc $(a^n - 1, a^m - 1) = (a^m - 1, a^r - 1)$, car $a^m - 1 \mid (a^m)^q - 1$. De même, si r_1 est le reste de la division euclidienne de m par r, on obtient $(a^m - 1, a^r - 1) = (a^r - 1, a^{r_1} - 1)$, et ainsi de suite. La suite des exposants est la suite obtenue en appliquant l'algorithme d'Euclide à n et m ; on obtient donc $(a^n - 1, a^m - 1) = (a^{(n,m)} - 1, a^0 - 1) = a^{(n,m)} - 1$.

- Définition des congruences -

Exercice 3 Pour quels entiers naturels n a-t-on $13 \mid 14^n - 27$.

Solution de l'exercice 3 Il suffit de remarquer que $14 = 13 + 1$ et que dans le développement de $(13 + 1)^n$, 13 apparaît toujours en facteur sauf pour le dernier terme, qui est 1.
Ainsi $13 \mid 14^n - 27 \iff 13 \mid 1 - 27 = -26$ ce qui est toujours vérifié.

L'exercice précédent est ici simplement pour illustrer la notion de congruence. On dit que deux entiers a et b sont congrus modulo un entier n, et on note $a \equiv b[n]$, si n divise $b - a$. Dans ce cas, si la question est de savoir si une certaine expression faisant intervenir a est divisible par un entier n, on peut remplacer a par b dans l'expression (pour la simplifier en général), sans modifier le résultat.

En effet, l'addition et la multiplication des entiers sont compatibles avec les congruences. Plus précisément, si $a \equiv b[n]$, alors $a + c \equiv b + c[n]$, $ac \equiv bc[n]$. On calcule donc modulo n comme on calcule dans les entiers, en ajoutant la règle $n = 0$. On note $\bar{a}$ la classe d'équivalence de a modulo n, qui est l'ensemble des entiers congrus à a modulo n. Un élément de cet ensemble est appelé un représentant de $\bar{a}$, et on peut sommer et multiplier des classes comme on le fait avec leurs représentants. On note $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ l'ensemble des classes d'équivalences modulo n, muni des opérations $+$ et $\times$, vérifiant les lois de compatibilité usuelles (associativité, distributivité, commutativité). On dit que $\mathbb{Z}/n\mathbb{Z}$, muni de ces deux opérations, est un anneau commutatif.

- Inversibilité modulo n -

Après avoir dit qu'on pouvait multiplier modulo n, une question naturelle est de savoir si on peut diviser des classes d'équivalence. Autrement dit, si $a \in \mathbb{Z}$, existe-t-il $a' \in \mathbb{Z}$ tel que $aa' \equiv 1[n]$ (on dira que a ou $\bar{a}$ est inversible modulo n et que $\bar{a}'$ est l'inverse de $\bar{a}$ dans $\mathbb{Z}/n\mathbb{Z}$). En revenant à la définition, cela revient à demander s'il existe $a', n' \in \mathbb{Z}$ tels que $aa' + nn' = 1$. La réponse est donnée par le théorème de Bézout :

Théorème 1 (Bézout)**.** Si $d = (a, b)$, alors il existe des entiers u et v tels que $au + bv = d$. Il est clair par ailleurs que d divise tout entier de la forme $au + bv$, donc la réponse à notre question est que a est inversible modulo n si et seulement si a et n sont premiers entre eux.

Voyons comment trouver l'inverse de $\bar{a}$, c'est-à-dire comment trouver a', quand a et n sont bien premiers entre eux. On appelle combinaison linéaire

entière de a et b tout nombre de la forme $au+bv$ avec u et v des entiers, qu'on appelle les coefficients de la combinaison linéaire. Notre but est de trouver la plus petite combinaison linéaire strictement positive de a et n, qui doit être 1. Pour cela, on applique simplement l'algorithme d'Euclide, qui donne une suite de restes (r_i) et de quotients (q_i) tels que $r_0 = a$, $r_1 = n$, $r_{i-1} = q_i r_i + r_{i+1}$, $r_k = 1$ et on remplace formellement r_0 par a et r_1 par n : $r_2 = a - q_1 n$, $r_3 = n - q_2(a - q_1 n) = a(-q_2) + n(1 + q_1 q_2)$, et ainsi de suite jusqu'à $1 = aa' + nn'$.

Exemple 2. Pour inverser 37 modulo 53, on écrit $16 = 53-37$, $5 = 37-2\times 16 = 3 \times 37 - 2 \times 53$, $1 = 16 - 3 \times 5 = (-10) \times 37 + 7 \times 53$ donc -10 est inverse de 37 modulo 53.

On note $\mathbb{Z}/n\mathbb{Z}^*$ l'ensemble des classes inversibles de $\mathbb{Z}/n\mathbb{Z}$. La fonction indicatrice d'Euler est définie par $\phi(n) := \mathrm{Card}(\mathbb{Z}/n\mathbb{Z}^*)$. On remarque que si n est premier, tout nombre non multiple de n est premier avec n donc toutes les classes sont inversibles sauf celle de 0, et en particulier, $\phi(n) = n - 1$.

Exercice 4 (Théorème de Wilson) Soit $N > 1$ un entier naturel, montrer que $(N-1)! \equiv -1[N]$ si et seulement si N est premier.

Solution de l'exercice 4 Si N est composé, il existe deux entiers naturels $a, b > 1$ tels que $N = ab$ et si $a \neq b$, comme $a, b < N$, on a $(N-1)! \equiv 0[N]$. Si $a = b$, $N = a^2$ et $2a \leqslant N - 1$ sauf si $N = 4$, et alors $(N-1)! \equiv 0[N]$. Si $N = 4$, $6 \not\equiv -1[4]$. Si N est premier, on calcule $(N-1)!$ en regroupant chaque terme avec son inverse. On obtient ainsi un produit de paires d'inverses, sauf pour 1 et -1 qui sont leurs propres inverses. Ce sont les seuls car si $x \equiv x^{-1}[N]$ alors $x^2 - 1 \equiv 0[N]$ donc $(x-1)(x+1) \equiv 0[N]$ donc $x \equiv \pm 1[N]$ car N est premier. Ainsi, les produits de paires d'inverses se simplifient et il reste $(N-1)! \equiv -1[N]$.

Exercice 5 Montrer que pour tout p premier, l'équation $6n^2 + 5n + 1 \equiv 0[p]$ a toujours des solutions.

Solution de l'exercice 5 Si $p = 2$ ou $p = 3$, $n = 1$ donne une solution. Sinon, on peut résoudre comme on le fait dans les réels : on prend la racine du discriminant sans mal car c'est 1, et on obtient $n = \frac{-5 \pm 1}{12}$ (12 est inversible modulo p).

- Lemme chinois -

Soit a, b, n trois entiers, d un diviseur de n, si $a \equiv b[n]$ alors $a \equiv b[d]$ car d divise n qui divise $a - b$. On a donc une fonction « naturelle »de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/d\mathbb{Z}$ qui à $\bar{k}$ associe $\bar{k}$. Elle est compatible avec l'addition et la multiplication.

Théorème 3. (Lemme chinois) Soit a et b deux entiers premiers entre eux, alors la fonction

$$\begin{cases} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \bar{k} & \longmapsto & (\bar{k}, \bar{k}) \end{cases}$$

est bijective.

De plus, elle est compatible avec l'addition et la multiplication.

Démonstration. On démontre la bijectivité. Comme les ensembles en question sont de même cardinal, il suffit de montrer l'injectivité. Il faut montrer que si n et m sont deux entiers tels que $n \equiv m[a]$ et $n \equiv m[b]$, alors $n \equiv m[ab]$. C'est le cas car a et b divisent $n - m$ et comme a et b sont premiers entre eux, ab divise $n - m$. □

Cela signifie que pour calculer dans $\mathbb{Z}/ab\mathbb{Z}$, on peut se ramener à calculer dans $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$, et réciproquement. On utilise le lemme chinois en particulier pour dire qu'un système de congruences modulo $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$ est équivalent à une congruence modulo $\mathbb{Z}/ab\mathbb{Z}$, via la bijection.

Exercice 6 On considère le plan muni d'un repère orthonormé d'origine O. On dit qu'un point M est invisible s'il existe un point à coordonnées entières sur $]OM[$. Montrer que pour tout entier naturel L il existe un carré de côté L, parallèle aux axes, tel que tous les points à coordonnées entières dans le carré soient invisibles.

Solution de l'exercice 6 Un point $M = (a, b) \in \mathbb{Z}^2$ est invisible si $\gcd(a, b) > 1$ car si $d \neq 1$ divise a et b, $(\frac{a}{d}, \frac{b}{d})$ est sur $]OM[$. Si on se donne $(p_{i,j})_{0 \leqslant i,j \leqslant L}$ des nombres premiers deux à deux distincts, alors d'après le lemme chinois il existe des entiers a et b tels que pour tous $0 \leqslant i, j \leqslant L$, $a \equiv -i[p_{i,j}]$ $b \equiv -j[p_{i,j}]$. Alors $\gcd(a + i, b + j) \geqslant p_{i,j} > 1$ donc tous les points $(a + i, b + j)$ sont invisibles, et le carré de côté L dont le coin inférieur gauche est (a, b) répond au problème.

Le théorème chinois permet de montrer directement la multiplicativité de l'indicatrice d'Euler, car la bijection se restreint en une bijection entre $\mathbb{Z}/ab\mathbb{Z}^*$ et $\mathbb{Z}/a\mathbb{Z}^* \times \mathbb{Z}/b\mathbb{Z}^*$, d'où l'on déduit que pour a et b premiers entre eux, $\phi(ab) = \phi(a)\phi(b)$. Par récurrence, on voit alors que si $n = \prod_i p_i^{\alpha_i}$ est la décomposition en facteurs premiers de n, alors $\phi(n) = \prod_i \phi(p_i^{\alpha_i}) = \prod_i p_i^{\alpha_i - 1}(p_i - 1)$ car le nombre d'entiers naturels premiers avec p^k inférieurs à p^k est $p^k - p^{k-1}$ donc $\phi(p^k) = p^{k-1}(p - 1)$.

- Ordre d'un élément -

Si $a \in \mathbb{Z}/n\mathbb{Z}^*$, en considérant l'ensemble des puissances de a dans $\mathbb{Z}/n\mathbb{Z}$, on voit par principe des tiroirs que deux d'entre elles sont égales, donc il existe des entiers $k > l$ tels que $a^k \equiv a^l[n]$ d'où $a^{k-l} \equiv 1[n]$. En particulier, il existe un plus petit entier naturel non nul $w(a)$ tel que $a^{w(a)} \equiv 1[n]$ qu'on appelle l'ordre de a (modulo n).

Théorème 4 (Euler)**.** Si $a \in \mathbb{Z}/n\mathbb{Z}^*$ alors $a^{\phi(n)} \equiv 1[n]$.

Corollaire 5 (petit théorème de Fermat)**.** Si $a \in \mathbb{Z}/p\mathbb{Z}^*$ avec p premier, alors $a^{p-1} \equiv 1[n]$.

Démonstration. La multiplication par a effectue une permutation de $\mathbb{Z}/n\mathbb{Z}^*$ (c'est une injection car a est inversible, donc une bijection par égalité des cardinaux). On a donc
$\prod_{r\in\mathbb{Z}/n\mathbb{Z}^*} r \equiv \prod_{r\in\mathbb{Z}/n\mathbb{Z}^*} ar \equiv a^{\phi(n)} \prod_{r\in\mathbb{Z}/n\mathbb{Z}^*} r[n]$ donc en simplifiant, on obtient $a^{\phi(n)} \equiv 1[n]$.

□

Exercice 7 Trouver tous les entiers naturels n tels que n divise $2^n - 1$.

Solution de l'exercice 7 Le nombre 1 convient. Soit p le plus petit diviseur premier de $n \neq 1$. Comme $2^n \equiv 1[n]$, on a aussi $2^n \equiv 1[p]$, et par le petit théorème de Fermat, $2^{p-1} \equiv 1[p]$, donc l'ordre de 2 modulo p divise le PGCD de n et $p-1$, donc vaut 1 car $p-1$ est plus petit que le plus petit nombre premier divisant n, donc est premier avec n. Ainsi $2 \equiv 1[p]$ donc $p = 1$, absurde. Ainsi, 1 est la seule solution.