le cnam

Algèbre de Boole, probabilités et arithmétique

Cours 7 Congruences

• Calculer "*modulo*" [du latin *modulus*, relatif à la mesure]

On se donne un entier n supérieur ou égal à 1 et deux entiers relatifs a et b. On dit que "a est congru à b *modulo* n" et on note $a \equiv b \pmod{n}$ si et seulement si l'entier $(b-a)$ est un multiple de n, c'est à dire s'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$.

Par exemple, on a $6 \equiv 0 \pmod{6}$, $7 \equiv 1 \pmod{6}$ et $5 \equiv -1 \pmod{6}$.

En pratique, le cas $n = 1$ ne donne aucune information, et on choisit $n \geq 2$. Ainsi, pour $n = 2$, la relation $a \equiv 0 \pmod{2}$ signifie que a est un entier pair alors que la condition $a \equiv 1 \pmod{2}$ indique que l'entier a est impair.

• Lien avec la division euclidienne

Si on divise l'entier $a \in \mathbb{Z}$ par l'entier $n \geq 1$, on peut écrire $a = nq + r$ avec le reste r tel que $0 \leq r \leq n-1$. On en déduit immédiatement que $a \equiv r \pmod{n}$; un entier est toujours congru modulo n au reste de la division euclidienne de cet entier par le nombre n. En conséquence, deux nombres sont congus *modulo* n si et seulement si ils ont le même reste dans leur division euclidienne par n.

• Premières propriétés de la relation *modulo*

On a les propriétés fondamentales suivantes, très analogues à celles de l'égalité :

réflexivité : $a \equiv a \pmod{n}$,

symétrie : si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$,

transitivité : si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$.

• Compatibilité de la relation *modulo* avec l'addition

On peut ajouter terme à terme les relations de congruences :

si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a + c \equiv b + d \pmod{n}$. Il suffit d'écrire la définition : il existe deux entiers k et ℓ de sorte que $b = a + kn$ et $d = c + \ell n$. Alors $b + d = a + c + (k + \ell)\, n$ ce qui établit le résultat.

• Compatibilité de la relation *modulo* avec la multiplication

On peut multiplier terme à terme les relations de congruences :

si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $ac \equiv bd \pmod{n}$. Avec les notations du paragraphe précédent, on multiplie maintenant les deux égalités $b = a + kn$ et $d = c + \ell n$:

$bd = (a + kn)\,(c + \ell n) = ac + (kc + \ell a + k\ell n)\, n$ et le produit ac est congru à bd *modulo* n.

François Dubois, novembre 2023.

- Compatibilité de la relation *modulo* avec l'exponentiation

On peut élever à une même puissance entière positive deux nombres congrus *modulo* n : si $\ell \in \mathbb{N}$ et $a \equiv b \pmod{n}$, alors $a^\ell \equiv b^\ell \pmod{n}$. C'est clair si $\ell = 0$ ou $\ell = 1$. Si $\ell = 2$, compte tenu du paragraphe précédent, on a $a \times a \equiv b \times b \pmod{n}$, c'est à dire $a^2 \equiv b^2 \pmod{n}$. La preuve se mène alors par récurrence sur l'entier ℓ.

- Étude de l'exemple $n = 6$

On ne manipule essentiellement en pratique des nombres entiers compris entre 0 et 6. La table d'addition permet d'expliciter les opposés modulo 6 : $1+5 \equiv 0$, $2+4 \equiv 0$ et $3+3 \equiv 0$. Pour la multiplication, on a bien sûr $0 \times a \equiv 0$ pour tout a et $1 \times a \equiv a$. On a également $2 \times 2 \equiv 4$ et la curieuse relation $2 \times 3 \equiv 0$. Cette relation est liée au fait que 2 est un diviseur de 6. On dit que les nombres 2 et 3 sont des "diviseurs de zéro" quand on calcule *modulo* 6. On a ensuite $2 \times 4 \equiv 2$, $2 \times 5 \equiv 4$, $3 \times 3 \equiv 3$, $3 \times 4 \equiv 0$, $3 \times 5 \equiv 3$, $4 \times 4 \equiv 4$ et $4 \times 5 \equiv 2$. Enfin, $5 \times 5 \equiv 1$. Seuls les nombres 1 et 5 ont un "inverse" *modulo* 6, c'est à dire à un multiple de 6 près ; on a en effet les congruences $1 \times 1 \equiv 1$ et $5 \times 5 \equiv 1$.

- Éléments inversibles *modulo* n

On se donne un entier $n \geq 2$ et un entier relatif $a \in \mathbb{Z}$. On dit que le nombre a est "inversible *modulo* n" si et seulement si il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$.
Par exemple, nous avons vu au paragraphe précédent que 5 est inversible *modulo* 6. Mais 2 n'est pas inversible *modulo* 6 ainsi que nous pouvons le prouver par l'absurde. Si il existe un entier $b \in \mathbb{Z}$ tel que $2b \equiv 1 \pmod{6}$, nous multiplions cette congruence par 3 : Alors
$(2b) \times 3 \equiv 3 \pmod{6}$ donc $0 \equiv 3 \pmod{6}$ ce qui est faux et montre la contradiction.
De façon générale, un diviseur de zéro n'est pas inversible. Le théorème qui suit permet de caractériser les éléments inversibles *modulo* n.

Théorème. On se donne un entier $n \geq 2$ et un entier relatif $a \in \mathbb{Z}$. Cet entier a est inversible *modulo* n si et seulement si a et n sont premiers entre eux :
$\big(\exists b \in \mathbb{Z}, ab \equiv 1 \pmod{n}\big) \Leftrightarrow (a \wedge n = 1)$.
La preuve repose sur l'identité de Bézout. Si a est inversible *modulo* n, il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$. Cette relation signifie qu'il existe $k \in \mathbb{Z}$ tel que $ab = 1 + kn$, relation qu'on peut aussi écrire $ab + n(-k) = 1$. Nous venons de mettre en évidence une identité de Bézout entre les entiers a et n, qui sont donc premiers entre eux. Réciproquement, si a et n sont premiers entre eux, il existe deux entiers relatifs b et v tels que $ab + nv = 1$. On a donc $ab = 1 + (-v)n$ et $ab \equiv 1 \pmod{n}$. Le résultat est établi.

- Une propriété des coefficients binômiaux dans le cas d'un nombre premier

On se donne un nombre premier p et un entier k compris entre 1 et $(p-1)$. On rappelle que le nombre de combinaisons k à k de p objets est noté $\binom{p}{k}$. Avec les hypothèses faites plus haut, le nombre premier p divise les coefficients binômiaux $\binom{p}{k}$: $p \,|\, \binom{p}{k}$.

Ce critère de divisibilité est explicite quand on regarde le triangle de Pascal

0	1							
1	1	1						
2 est premier	1	2	1					
3 est premier	1	3	3	1				
4	1	4	6	4	1			
5 est premier	1	5	10	10	5	1		
6	1	6	15	20	10	6	1	
7 est premier	1	7	21	35	35	21	7	1

Pour prouver cette propriété, on rappelle d'abord que $k!\,\binom{p}{k} = p\,(p-1)\,...\,(p-(k-1))$. Donc p divise le produit $k!\,\binom{p}{k}$. Si $p=2$, la seule valeur possible pour l'entier k est $k=1$ et la propriété est vraie. Si $p \geq 3$, on a $k!\,\binom{p}{k} = 2\times 3\times ...\times k\times\binom{p}{k}$. On a vu au chapitre précédent que le nombre premier p est premier à tout entier k compris entre 1 et $(p-1)$. Comme p est premier à 2 et que p divise le produit $2\times\left[3\times ...\times k\times\binom{p}{k}\right]$, le lemme de Gauss entraîne que p divise l'entier $3\times ...\times k\times\binom{p}{k}$. On recommence de la même façon pour le nombre 3 et de proche en proche pour tous les entiers jusqu'à l'entier k. À la fin de ces applications successives du lemme de Gauss, on a établi que le nombre premier p divise le coefficient binômial $\binom{p}{k}$.

- Petit théorème de Fermat (Pierre de Fermat, $\simeq$ 1605-1665)

On se donne un nombre premier p et un nombre entier $a \in \mathbb{Z}$. Alors $a^p \equiv a \pmod{p}$. En d'autres termes, le nombre $a^p - a$ est toujours un multiple de p.

Par exemple pour $p=2$, tout entier pair est congru à 0 *modulo* 2 et tout entier impair est congru à 1 *modulo* 2. En particulier, $-1 \equiv 1 \pmod{2}$. On a alors facilement $0^2 \equiv 0 \pmod{2}$ et $1^2 \equiv 1 \pmod{2}$. Pour tout nombre entier pair a, on a $a \equiv 0 \pmod{2}$ donc
$a^2 \equiv 0^2 \equiv 0 \equiv a \pmod{2}$ et pour tout entier impair a, $a^2 \equiv 1^2 \equiv 1 \equiv a \pmod{2}$, ce qui montre la propriété dans ce cas fondamental.

On prend d'abord le temps de vérifier que la propriété est vraie pour $p=7$ par exemple. Dans ce cas, tout entier est congru à l'un des nombres 0, 1, 2, 3, 4, 5 et 6 *modulo* 7. On a $0^7 = 0$ et $1^7 = 1$ donc la propriété est vraie pour ces deux entiers. On a ensuite $2^3 = 8$ donc $2^3 \equiv 1$, puis $2^6 = (2^3)^2 \equiv 1^2 \equiv 1$. On en déduit que $2^7 = 2^6 \times 2 \equiv 1\times 2 \equiv 2$ *modulo* 7. On a ensuite $3^2 = 9 \equiv 2$ donc $3^3 \equiv 3\times 2 \equiv 6 \equiv -1 \pmod{7}$ puis $3^6 = (3^3)^2 \equiv (-1)^2 \equiv 1$. Donc $3^7 = 3^6\times 3 \equiv 1\times 3 \equiv 3$ *modulo* 7. Le nombre 4 se traite de la même manière : $4^2 = 16 \equiv 2$ donc $4^6 \equiv 2^3 \equiv 8 \equiv 1$ *modulo* 7 et $4^7 = 4^6 \times 4 \equiv 1\times 4 \equiv 4 \pmod{7}$. Il est utile de remarquer que $5 \equiv -2$ *modulo* 7. Donc $5^3 \equiv (-2)^3 \equiv -8 \equiv -1$. Puis $5^6 \equiv (5^3)^2 \equiv (-1)^2 \equiv 1$; enfin $5^7 = 5^6 \times 5 \equiv 1\times 5 \equiv 5 \pmod{7}$. Last but not least, $6 \equiv -1$ *modulo* 7, donc $6^2 \equiv 1 \pmod{7}$ et $6^6 \equiv 1^3 \equiv 1$. On en déduit que $6^7 = 6^6 \times 6 \equiv 1\times 6 \equiv 6$ *modulo* 7.

On commence par prouver la propri $a^p \equiv a \pmod{p}$ par récurrence pour $a \in \mathbb{N}$. Il est clair que si $a=0$, on a $a^p = 0 = a$ donc $a^p \equiv a \pmod{p}$. Si on suppose la propriété vraie pour l'entier a, est-elle vraie pour l'entier suivant $(a+1)$? On développe $(a+1)^p$ avec la formule du binôme de Newton : $(a+1)^p = a^p + \left[\sum_{k=1}^{p-1}\binom{p}{k}a^k\right] + 1^p$. Or pour tout entier

$k = 1, 2, ... (p-1)$, le coefficient binômial $\binom{p}{k}$ est divisible par p. Donc il en est de même de la somme $\big[\sum_{k=1}^{p-1} \binom{p}{k} a^k\big]$. On en déduit que $(a+1)^p \equiv a^p + 1 \pmod{p}$. On utilise enfin l'hypothèse de récurrence $a^p \equiv a \pmod{p}$. On en déduit $(a+1)^p \equiv a+1 \pmod{p}$ et la propriété est démontrée pour tous les entiers positifs.
Si a est un entier négatif, on peut l'écrire $a = -\alpha$ avec $\alpha \in \mathbb{N}$. Si $p = 2$, $-1 \equiv 1 \pmod{2}$ et $a^p \equiv a$ *modulo* 2. Si p est un nombre premier supérieur ou égal à 3, il est impair et $(-1)^p = -1$ donc $(-1)^p \equiv -1 \pmod{p}$. On en déduit $a^p = (-1)^p \alpha^p \equiv -\alpha^p \equiv -\alpha \pmod{p}$ d'après ce qui a été fait dans le cas des entiers positifs. Donc $a^p \equiv -\alpha \equiv a$ *modulo* p.

• Second énoncé du petit théorème de Fermat

On se donne un nombre premier p et un entier $a \in \mathbb{Z}$. Si a et p sont premiers entre eux, alors $a^{p-1} \equiv 1 \pmod{p}$.
Nous avons clairement utilisé cette propriété dans l'étude exhaustive du cas $p = 7$.
La preuve est une conséquence du petit théorème de Fermat. Nous savons que a^p est congru à a *modulo* p, donc p divise le produit $a\,(a^{p-1}-1)$. Comme a et p sont premiers entre eux par hypothèse, le lemme de Gauss entraîne que l'entier p divise $(a^{p-1}-1)$. En d'autres termes, le nombre a^{p-1} est congru à 1 *modulo* p, ce qui établit le résultat.

• Généralisation du petit théorème de Fermat

On se donne deux nombres premiers différents p et q et un entier a premier au produit $n = pq$. Alors $a^{(p-1)\,(q-1)} \equiv 1 \pmod{n}$.
On pose $c = a^{(p-1)\,(q-1)}$. Si a est premier à $n = pq$, il existe deux entiers u et v de sorte que $a\,u + p\,q\,v = 1$. On peut lire cette relation sous la forme $a\,u + p\,(q\,v) = 1$ et cette identité de Bézout montre que a et p sont premiers entre eux. De façon analogue, on peut lire la relation précédente sous la forme $a\,u + q\,(p\,v) = 1$ et les entiers a et q sont premiers entre eux. Comme a et p sont premiers entre eux, le petit théorème de Fermat montre que $a^{p-1} \equiv 1 \pmod{p}$. On en déduit $c = \big(a^{p-1}\big)^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p}$. De même, a et q sont premiers entre eux et $a^{q-1} \equiv 1 \pmod{q}$ avec le petit théorème de Fermat. Il vient alors
$c = \big(a^{q-1}\big)^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{q}$. Nous venons d'établir que le nombre c est congru à 1 *modulo* p et *modulo* q. Il existe donc deux entiers k et ℓ de sorte que $c = 1 + k\,p = 1 + \ell\,q$. En conséquence, $k\,p = \ell\,q$. Le nombre p divise le produit $q\,\ell$ et $p \wedge q = 1$ car p et q sont deux nombres premiers différents. Vu le lemme de Gauss, p divise ℓ et il existe un entier m tel que $\ell = p\,m$. On a finalement $c = 1 + p\,q\,m$ ce qui signifie que c est congru à 1 *modulo* pq et montre la propriété.

Dans le cas $p = 2$ et $q = 5$ par exemple, on a $p - 1 = 1$ et $q - 1 = 4$. On peut se convaincre que si a est premier à 10, $a^4 \equiv 1$ *modulo* 10. Nous laissons au lecteur le soin de le vérifier, sachant que les nombres premiers à 10 sont congrus à 1, 3, 7 ou 9 *modulo* 10.

Second exemple avec $p = 3$ et $q = 5$, donc $n = 15$. On a alors $p - 1 = 2$, $q - 1 = 4$. Si a est premier à 15, alors il suffit de vérifier que $a^8 \equiv 1 \pmod{15}$. On compte cette fois 8 nombres entiers positifs inférieurs à 15 et premiers à 15 : 1, 2, 4, 7, 8, 11, 13 et 14. Il suffit d'effectuer le calcul *modulo* 15 de ces huit nombres élevés à la puissance 8.

- Indicatrice d'Euler (Leonhard Euler, 1707-1783)

La généralisation précédente est le premier pas dans la construction de l'indicatrice d'Euler $\varphi(n)$. Pour n entier supérieur ou égal à 1, $\varphi(n)$ désigne le nombre d'entiers premiers à n compris entre 1 et n. Nous avons établi à la leçon précédente que si $n = p$ est un nombre premier, alors $\varphi(p) = p-1$.
On peut démontrer la propriété générale qui exprime que l'indicatrice d'Euler est une fonction multiplicative : si les entiers n et m sont premiers entre eux, alors $\varphi(nm) = \varphi(n)\,\varphi(m)$. On en déduit que si l'entier n est de la forme $n = pq$ pour deux nombres premiers différents, alors $\varphi(pq) = (p-1)\,(q-1)$.

Théorème. Généralisation du petit théorème de Fermat par Euler.
On se donne un entier n supérieur ou égal à 1 et $a \in \mathbb{Z}$ un entier quelconque. Si a et n sont premiers entre eux, alors $a^{\varphi(n)} \equiv 1$ *modulo* n.
Nous aurons seulement besoin dans la suite de ce cours du cas où l'entier n est de la forme $n = pq$ pour deux nombres premiers différents : $a^{(p-1)\,(q-1)} \equiv 1 \pmod n$ si $a \wedge n = 1$.

Exercices

- Une variation sur l'identité de Bézout

a) Montrer que si les entiers a et b sont premiers entre eux, il en est de même des entiers $(a+b)$ et ab. [travailler avec l'identité de Bézout]
b) Réciproquement, démontrer que si les entiers $(a+b)$ et ab sont premiers entre eux, alors a et b sont premiers entre eux. [Bézout encore et toujours...]

- Parité

On se donne un entier $n \in \mathbb{N}$.
a) Montrer que l'expression $m = 3n^4 + 5n + 1$ est toujours un nombre impair.
b) En déduire que l'entier m n'est pas divisible par un nombre entier de la forme $n\,(n+1)$.

- Diviseur

Montrer que si $a \in \mathbb{Z}$, le nombre 6 divise le produit $a\,(a^2-1)$.

- Divisibilité d'un grand nombre

Le nombre entier $x = 2^{37} + 3^{37} - 5$ est un grand nombre entier de l'ordre de $4,50 \times 10^{17}$. Il est à l'extrême limite de la précision des calculs qu'un ordinateur de 64 bits peut effectuer sans erreur avec des nombres entiers.
a) Montrer que le nombre x défini plus haut est pair.
b) Montrer que 37 est un nombre premier
c) Montrer que les nombres $2^{36} - 1$ et $3^{36} - 1$ sont divisibles par 37.
d) En déduire que $x = 2^{37} + 3^{37} - 5$ est divisible par 37.
e) Démontrer que $x = 2^{37} + 3^{37} - 5$ est divisible par 74.

- Somme de carrés

On se donne un entier n qui est la somme de deux carrés. Montrer qu'alors le reste de la division de n par 4 n'est jamais égal à 3.

- Division par 8

a) Montrer que si n est un entier impair, le nombre $(7^n + 1)$ est divisible par 8.

b) Quel est le reste de la division de $(7^n + 1)$ par 8 si n est un entier pair ? [2]

- Une division avec un dividende très grand

On pose $g = 100^{1000}$.

a) Combien le nombre g comporte-t-il de zéros dans sa représentation décimale ?

b) Pourquoi le nombre 13 est-il premier ?

c) Quel est le reste de la division de 100^{1000} par 13 ? [9]