DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Exercices

AUTEUR : Louis NEBOUT
STAGE : Montpellier 2013

Congruences

Cette séance parlait des congruences. L'essentiel de ce qui a été vu pendant la séance est traité sur le cours du site d'Animath, dans le chapitre 3. Je ne vais donc pas refaire le cours entier, mais juste donner un résumé, en renvoyant vers le cours pour plus de précisions. L'adresse de ce cours est à l'adresse http ://www.animath.fr/spip.php ?article255.

J'ai commencé par définir les congruences (définition 3.1.1), en comparant congruences modulo un entier 12 avec les heures écrites sur une horloge à 12 chiffres, puis par analogie en comparant les congruences modulo un entier n quelconque avec les heures écrites autour d'une hypothétique horloge à n chiffres.

J'ai ensuite insité sur la dernière propriété du cours : on peut « additionner » et « multiplier » les modulo. Intuitivement, la propriété sur l'addition peut se visualiser en remarquant que avancer de 15 heures à partir d'une position donnée sur l'horloge à 12 heures, c'est la même chose que d'avancer de 3 heures. Pour visualiser la propriété sur la multiplication, une idée est de regarder modulo 10 : un nombre est congru à son dernier chiffre modulo 10, et on sait bien que pour trouver le dernier chiffre d'un produit de deux nombres, il suffit d'examiner le produit des deux derniers chiffres.

Je suis ensuite passé à la partie 3.2, sur les critères de divisibilité. Si en entier s'écrit $\overline{abcde}$ en base 10, alors il vaut $a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + e$. Si on connaît les valeurs prises par la suite $(10)^n$ modulo k, alors on aura une méthode rapide pour trouver la valeur de $\overline{abcde}$ modulo k.

Par exemple, avec $k = 7$, on vérifie que $10 \equiv 3\,[7]$, $10^2 \equiv 2\,[7]$, $10^3 \equiv -1\,[7]$,

et $10^4 \equiv -3\,[7]$. Ainsi, on aura

$$\begin{aligned}\overline{abcde} &\equiv a\cdot(-3)+b\cdot(-1)+c\cdot 2+d\cdot 3+e\,[7]\\ &\equiv -3a-b+2c+3d+e\,[7]\,.\end{aligned}$$

Un exemple concret : $\overline{17255} \equiv -3-7+4+15+5\,[7]$, et donc il est divisible par 7. On peut fabriquer autant de tels critères que l'on veut.

On voit sur cet exemple la grande force de la notion de congruence : elle permet de remplacer des calculs sur des grands nombres par des calculs sur des nombres bien plus petits, donc plus faciles. Un exemple spectaculaire est donné par l'exercice suivant. Il utilise une astuce classique, due au fait que 10 est congru à 1 modulo 9 : un nombre est toujours congru à la somme de ses chiffres modulo 9.

Exercice 1 Calculer la somme des chiffres de la somme des chiffres de la somme des chiffres de $A := 4444^{4444}$.

Solution de l'exercice 1 Notons $S(n)$ la somme des chiffres d'un entier n. Alors, notre astuce dit que pour tout n, $S(n) \equiv n\,[9]$. Ainsi, $S(S(S(A))) \equiv A\,[9]$. Calculons donc A modulo 9. On a $4444 \equiv 4+4+4+4 \equiv -2\,[9]$, il faut donc calculer $(-2)^{4444}$ modulo 9. On remarque que $(-2)^3 \equiv 1\,[9]$. On en déduit que $(-2)^{3k+i} \equiv ((-2)^3)^k \cdot (-2)^i \equiv (-2)^i\,[9]$. En particulier, comme $4444 \equiv 4+4+4+4 \equiv 1\,[3]$, donc $(-2)^{4444} \equiv (-2) \equiv 7\,[9]$.

Ainsi, on connaît $S(S(S(A)))$ modulo 9. Pour trouver sa vraie valeur, l'idée à avoir est que $S(n)$ est en général beaucoup plus petit que n. Ainsi, $S(S(S(A)))$ est beaucoup beaucoup beaucoup plus petit que A, et avec un peu de chance il sera suffisamment petit pour pouvoir le déterminer. On écrit donc que $A \leqslant (10^4)^{5000} = 10^{20000}$, donc A a au plus 20000 chiffres, donc $S(A) \leqslant 20000 \cdot 9 \leqslant 200000$. Donc $S(S(A)) \leqslant 1+9\cdot 5 = 46$, puis $S(S(S(A))) \leqslant 3+9 = 12$. Or il vaut 7 modulo 9, c'est donc nécessairement 7.

La seconde partie de la séance fut consacrée a l'étude des équations linéaires modulo n. Nous avons examiné les équations $5x \equiv 10\,[16]$ et $5x \equiv 10\,[15]$. Dans chaque cas, on est tenté de « diviser par 5 ». CELA N'A AUCUN SENS, ET IL NE FAUT SURTOUT PAS LE FAIRE. Les seules opérations que nous avons le droit de faire modulo n sont l'addition et la multiplication, n'allez pas inventer d'autres règles comme une éventuelle division par 5, dans la majorité des cas, ce sera faux.

Résolvons explicitement ces systèmes. Pour le premier, l'équation se réecrit $5x = 16k + 10$. En particulier 5 doit divise $16k$, or il est premier avec 16, il

divise donc k par lemme de Gauss : on écrit $k = 5k'$ puis on divise par 5, et il reste $x = 16k' + 2$. Réciproquement, on vérifie que les $x \equiv 2\,[16]$ conviennent : dans ce cas, la « division par 5 » aurait donc donné le bon résultat.

Pour le deuxième, il se réecrit $5x = 15k + 10$: on divise par 5 et $x = 3k + 2$. Réciproquement, les $x \equiv 2\,[3]$ sont solution. Dans ce cas, la « division par 5 » n'aurait pas marché.

Les résultats 3.1.2 et 3.1.3 du cours précisent tout cela. En fait, la « division par 5 » que l'on a envie de faire peut se voir comme une multiplication par $1/5$, et le théorème 3.1.2 dit précisément que, dans certains cas, on a une notion d'inverse modulo n. Ainsi, 5 possède un inverse modulo 16 (par exemple -3), on peut donc multiplier l'équation $5x \equiv 10\,[16]$ par -3, on obtient $x \equiv 5 \cdot (-3) \cdot x \equiv 10 \cdot (-3) \equiv 2\,[16]$. C'est là l'essence de la proposition 3.1.3. Par contre, 5 n'a pas d'inverse modulo 15 (si vous voulez le prouver, partez du fait que $5 \cdot 3 \equiv 0\,[15]$). Quand on examine la preuve de ces résultats, on remarque que c'est juste une utilisation du théorème de Bézout. En particulier, si on connaît un couple de Bézout pour les entiers c et N (c'est-à-dire x et y tels que $xc + yN = 1$), alors on connaît un inverse de c modulo N : x. La partie 2.3 du cours est donc fondamentale : elle explique comment, à partir de la division euclidienne, on peut construire des couples de Bézout. Ainsi, on dispose d'n algorithme très pratique pour déterminer les inverses modulo N.

Je suis ensuite passé aux systèmes de plusieurs équations, en donnant l'exemple du système $\begin{cases} x \equiv 5\,[7] \\ x \equiv 8\,[11] \end{cases}$. On peut résoudre ce système explicitement, ainsi la première équation nous permet d'écrire x sous la forme $7k + 5$, et ensuite on doit avoir $7k + 5 \equiv 8\,[11]$, autrement dit $7k \equiv 3\,[11]$ puis $k \equiv 2\,[11]$ en multipliant par l'inverse 8 de 7 modulo 11. Ainsi, k est de la forme $11k' + 2$, puis x est de la forme $7(11k' + 2) + 5$, c'est-à-dire $77k' + 19$. Réciproquement, ces nombres sont bien solutions.

En fait un théorème, appelé théorème chinois, 3.4.1 dans le cours, dit que ce genre de méthode est très générale : si m et n sont deux nombres premiers entres eux, si $um + vn = 1$ est une relation de Bézout entre ces deux entiers, alors les solutions du système $\begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n] \end{cases}$ sont exactement les nombres congrus à $s := umb + vna$ modulo mn. En effet, ce nombre est clairement solution (remarquez que $um \equiv 1\,[n]$, c'est le sens de la relation de Bézout), et si x est une autre solution, alors m et n divise $x - s$, donc leur produit divise $x - s$ (car m et n sont premiers entre eux), donc $x \equiv s\,[mn]$. Remarquez à nouveau

la grande utilité de l'algorithme d'Euclide : il permet de trouver le coefficients de Bézout, donc de résoudre directement de tels systèmes d'équations.